ExaRAID

Accusys RAID GUI
User's Manual

ExaRAID GUI USER'S GUIDE

Accusys
The RAID Architects

Accusys
The RAID Architects

Accusys RAID GUI
User's Manual

ExaRAID GUI

Version:1.6

ExaRAID

Notice

Product features and specifications described in this manual are subject to change without notice.

The manufacturer shall not be liable for any damage or loss of information resulting from the performance or use of the information contained herein.

Trademarks

Accusys and the names of Accusys products and logos referenced herein are either trademarks and/or service marks or registered trademarks and/or service marks of Accusys, Inc.

Microsoft, Windows, Windows NT, Windows 2000, Windows 2003, MS-DOS are either trademarks or registered trademarks of Microsoft Corporation. Intel and Pentium are registered trademarks of Intel Corporation. Other product and company names mentioned herein may be trademarks and/or service marks of their respective owners.

All contents of this manual are copyrighted by Accusys, Inc.

The information contained herein is the exclusive property of Accusys, Inc. and shall not be copied, transferred, photocopied, translated on paper, film, electronic media or computer-readable form, or otherwise reproduced in any way, without the explicit written permission of Accusys, Inc.

Manual version 1.6

© Copyright 2008 Accusys, Inc.

All rights reserved

About this manual

Congratulations on your purchase of the product. This controller allows you to control your RAID system through a user-friendly GUI, which is accessed through your web browser.

This manual is designed and written for users installing and using the RAID controller. The user should have a good working knowledge of RAID planning and data storage.

Symbols used in this manual

This manual highlights important information with the following icons:

CAUTION

This icon indicates the existence of a potential hazard that could result in personal injury, damage to your equipment or loss of data if the safety instruction is not observed.

NOTE

This icon indicates useful tips on getting the most from your RAID controller.

Company Contact

Accusys, Inc.

- 5F., No.38, Taiyuan St., Jhubei City, Hsinchu County 30265, Taiwan(R.O.C)
- Tel: +886-3-560-0288
- Fax: +886-3-560-0299
- http://www.accusys.com.tw/
- E-mail: sales@accusys.com.tw

Accusys U.S.A., Inc.

- 46710 Fremont Blvd. Fremont, CA 94538, U.S.A.
- Tel: +1-510-661-0800
- Fax: +1-510-661-9800
- Toll-free number: +1-866-277-5888
- http://www.accusys.com/
- E-mail: support@accusysusa.com

Accusys Korea, Inc.

- Baegang B/D 5F Shinsa-Dong 666-14 Kangnam-Gu, Seoul, Korea
- Tel: +82 (02) 6245-9052
- Fax: +82 (02) 3443-9050
- http://www.accusys.co.kr/
- E-mail: sales@accusys.co.kr

Accusys China(Beijing), Inc.

- No. 1701, Blk B, Horizon International Tower, No. 6 Zhichun Street, Haidian District, Beijing, ZIP: 100088, China
- http://www.accusys.com.cn
- Ftp://ftp.accusys.com.cn
- E-mail: sales@accusys.com.cn
- Tel: +86-10-82800080/81/82/83
- Fax: +86-10-82800784
- E-mail: kevinlee@accusys.com.cn

Accusys China(Shanghai), Inc.

- Room 701, No. 666, Kirin Tower, Gubei Road, Changning Area Shanghai, ZIP: 200336, China
- Tel: +86-21-6270-8599
- Fax: +86-21-6270-8580
- E-mail: sales@accusys.com.cn

Accusys EU B.V

- Orionweg 6, 4782 SC Moerdijk, The Netherlands
- Tel: +31 (0) 102995758
- Fax: +31 (0) 168358621
- http://www.accusyseu.com

- ftp://ftp.accusyseu.com
- E-mail: sales@accusyseu.com, support@accusyseu.com

Table of Contents

Chapter 1: Introduction

1.1 Overview 1-1
1.2 Key Features 1-2
1.3 How to Use This Manual 1-7
1.4 RAID Structure Overview 1-8
1.5 User Interfaces to Manage the RAID System 1-10
1.6 Initially Configuring the RAID System 1-11
1.7 Maintaining the RAID System 1-14

Chapter 2: Using the RAID GUI

2.1 Accessing the RAID GUI 2-1
2.1.1 Browser Language Setting 2-1
2.1.2 Multiple System Viewer 2-3
2.2 Monitor Mode 2-5
2.2.1 HDD state 2-6
2.2.2 Information icons 2-7
2.2.3 Rear side view 2-9
2.2.4 Login 2-11
2.3 SAS JBOD Enclosure Display (for SAS expansion controller only) 2-12
2.3.1 Rear side monitor of the SAS JBOD chassis 2-13
2.3.2 SAS JBOD Installation with RAID subsystem 2-13
2.3.3 Monitor mode 2-16
2.3.4 Information icons 2-17
2.3.5 SAS/SATA HDD information 2-17
2.4 Config Mode 2-18
2.5 Quick Setup 2-19
2.5.1 Performance profile 2-19
2.5.2 RAID setup 2-20
2.6 RAID Management 2-21
2.6.1 Hard disks 2-21
2.6.2 JBOD 2-23
2.6.3 Disk groups 2-25
2.6.4 Logical disks 2-27
2.6.5 Volumes 2-31
2.6.6 Snapshot Volumes 2-34
2.6.7 Storage provisioning 2-36
2.7 Maintenance Utilities 2-43
2.7.1 Expanding disk groups 2-43

2.7.2 Defragmenting disk groups 2-43
2.7.3 Changing RAID level / stripe size for logical disks 2-44
2.7.4 Expanding the capacity of logical disks in a disk group 2-45
2.7.5 Shrinking logical disks 2-46
2.7.6 Expanding volumes 2-46
2.7.7 Shrinking volumes 2-47
2.7.8 Cloning hard disks 2-47
2.7.9 Scrubbing 2-49
2.7.10 Regenerating the parity 2-50
2.7.11 Performing disk self test 2-50
2.7.12 Array roaming 2-51
2.7.13 Array recovery 2-52
2.7.14 Schedule task 2-54
2.7.15 Cache Configurations 2-54
2.7.16 Miscellaneous 2-55
2.8 Hardware Configurations 2-56
2.8.1 Hard disks 2-56
2.8.2 FC/SAS/SCSI ports 2-59
2.8.3 COM port 2-60
2.9 Event Management 2-61
2.9.1 Setting up the SMTP 2-61
2.9.2 Setting up the SNMP 2-62
2.9.3 Event logs 2-64
2.9.4 UPS 2-66
2.9.5 Miscellaneous 2-67
2.10 System Management 2-68
2.10.1 Restoring to factory settings 2-68
2.10.2 NVRAM configuration 2-68
2.10.3 Setting up the network 2-70
2.10.4 System Time 2-71
2.10.5 Security control 2-72
2.10.6 System information 2-73
2.10.7 Battery backup module 2-73
2.10.8 Update system firmware, boot code and external enclosure F/W 2-74
2.10.9 Restart or halt the controller 2-74
2.10.10 Miscellaneous 2-75
2.11 Performance Management 2-76
2.11.1 Hard disks 2-76
2.11.2 Cache 2-76
2.11.3 LUN 2-77
2.11.4 Storage port 2-78

Chapter 3: Using the LCD Console

3.1 Starting LCD Manipulation 3-1
3.1.1 Confirm password 3-1
3.2 LCD Messages 3-2
3.2.1 LCD layout 3-2
3.2.2 Status info 3-3
3.2.3 Emergent info 3-4
3.2.4 Background task messages 3-4
3.2.5 Hotkeys 3-5
3.3 Menu 3-6
3.3.1 Menu Tree 3-6
3.3.2 Creating an Array 3-6
3.3.3 Network Settings 3-7
3.3.4 Terminal Port Settings 3-7
3.3.5 System Settings 3-8
3.3.6 System Information 3-8

Chapter 4: Using the CLI Commands

4.1 Overview 4-1
4.1.1 Embedded CLI 4-1
4.1.2 Host-side Out-band CLI Utilities 4-2
4.1.3 Host-side In-band CLI Utilities 4-3
4.1.4 Conventions Overview 4-6
4.2 Basic RAID Management 4-7
4.2.1 Hard disks 4-7
4.2.2 JBOD disks 4-7
4.2.3 Disk groups 4-8
4.2.4 Spare and rebuild 4-9
4.2.5 Logical disks 4-10
4.2.6 RAID algorithms options 4-10
4.2.7 Volumes 4-11
4.2.8 Cache 4-12
4.3 RAID Maintenance Utilities 4-13
4.3.1 RAID attributes reconfiguration utilities 4-13
4.3.2 Data integrity maintenance utilities 4-14
4.3.3 Task priority control 4-15
4.3.4 Task schedule management 4-15
4.3.5 On-going task monitoring 4-16
4.3.6 Array and volume roaming 4-16
4.3.7 Array recovery utilities 4-17
4.4 Storage Presentation 4-17

4.4.1 Hosts 4-17
4.4.2 Host groups 4-18
4.4.3 Storage groups 4-19
4.4.4 Presentation planning 4-20
4.4.5 Selective storage presentation 4-20
4.4.6 Simple storage presentation 4-21
4.4.7 Symmetric-LUN storage presentation 4-21
4.5 Hardware Configurations and Utilities 4-22
4.5.1 Generic hard disk 4-22
4.5.2 SAS ports 4-24
4.5.3 SCSI ports 4-24
4.5.4 FC ports 4-25
4.5.5 Management network interface 4-26
4.5.6 Local terminal ports 4-27
4.5.7 Enclosure 4-28
4.5.8 Uninterruptible power supply 4-28
4.6 Performance management 4-29
4.6.1 Hard disks 4-29
4.6.2 Cache 4-29
4.6.3 LUN 4-29
4.6.4 Storage ports 4-30
4.7 Redundant Controller Configurations 4-31
4.7.1 Mirrored write cache control 4-31
4.7.2 Change preferred controller 4-31
4.7.3 Path failover alert delay 4-31
4.8 Event Management 4-31
4.8.1 NVRAM event logs 4-31
4.8.2 Event notification 4-32
4.8.3 Event handling 4-33
4.9 System Management 4-34
4.9.1 Configurations management 4-34
4.9.2 Time management 4-35
4.9.3 Administration security control 4-36
4.9.4 System information 4-37
4.9.5 Miscellaneous 4-37
4.10 Miscellaneous Utilities 4-39
4.10.1 Lookup RAID systems 4-39
4.10.2 Turn on/off CLI script mode 4-39
4.10.3 Get command list and usage 4-39
4.11 Configuration shortcuts 4-39
4.11.1 RAID quick setup 4-39

4.11.2 Performance profile 4-40
4.12 Snapshot 4-40

Chapter 5: Advanced Functions

5.1 Multi-Path IO Solutions 5-1
5.1.1 Overview 5-1
5.1.2 Benefits 5-1
5.1.3 Configuring MPIO Hosts and RAID Controller 5-2
5.1.4 Windows Multi-Path Solution: PathGuard 5-7
5.1.5 Linux Multi-Path Solution 5-12
5.1.6 MAC Multi-Path Solution 5-16
5.1.7 VMware ESX Server Multi-Path Solution 5-16
5.1.8 Sun Solaris 10 OS Multi-Path Solution 5-17
5.2 Multiple ID solutions 5-18
5.2.1 Overview 5-18
5.3 Redundant Controller 5-21
5.3.1 Overview 5-21
5.3.2 Controller Data Synchronization 5-23
5.3.3 Redundant-Controller System Configuration with MPIO 5-25
5.3.4 Controller and Path Failover/Failback Scenarios 5-34
5.4 Snapshot 5-38
5.4.1 Introduction 5-38
5.4.2 How Snapshot Works 5-39
5.4.3 How to Use Snapshots 5-41
5.4.4 Snapshot Utility and Scripting 5-45
5.5 Dynamic Capacity Management 5-48
5.5.1 Free chunk defragmentation 5-50
5.5.2 Logical disk shrink 5-51
5.5.3 Logical disk expansion 5-52
5.5.4 Disk group expansion 5-53
5.5.5 Volume expansion and shrink 5-54
5.5.6 Windows DiskPart Utility 5-55
5.6 RAIDGuard Central 5-58
5.6.1 Introduction 5-58
5.6.2 Deployment Overview 5-59
5.6.3 Installing the RAIDGuard Central 5-61
5.6.4 Uninstalling the RAIDGuard Central 5-62
5.6.5 Launching the RAIDGuard Central 5-62
5.6.6 RGC GUI Overview 5-65
5.6.7 RAID System Registration 5-67
5.6.8 RAID System Monitoring 5-71
5.6.9 Configuring MSN Event Notification 5-72

5.7 VDS Provider 5-73
5.7.1 Overview 5-73
5.7.2 Installing the VDS Provider 5-74
5.7.3 Uninstalling the VDS Provider 5-74
5.7.4 Using the VDS Provider Configuration Utility 5-74
5.7.5 VDS-Based RAID Management Software 5-76

Chapter 6: Troubleshooting

6.1 General Guidelines 6-1
6.2 Beeper 6-1
6.3 Performance Tuning 6-2
6.4 Hard Disks 6-5
6.5 User Interfaces 6-7
6.6 RAID Configuration and Maintenance 6-8
6.7 Redundant Controller and MPIO 6-10

Appendix A: Understanding RAID

A.1 RAID Overview A-1
A.2 RAID 0 ..... A-3
A.3 RAID 1 ..... A-4
A.4 RAID 3 ..... A-5
A.5 RAID 5 ..... A-6
A.6 RAID 6 ..... A-7
A.7 RAID 10 ..... A-8
A.8 RAID 30 ..... A-9
A.9 RAID 50 ..... A-10
A.10 RAID 60 ..... A-11
A.11 JBOD A-12
A.12 NRAID A-13

Appendix B: Features and Benefits

B.1 Overview B-1
B.2 Flexible Storage Presentation B-1
B.3 Flexible Storage Provisioning B-2
B.4 Comprehensive RAID Configurations B-3
B.5 Dynamic Configuration Migration B-4
B.6 Effective Capacity Management B-5
B.7 Adaptive Performance Optimization B-6
B.8 Proactive Data Protection B-8
B.9 Fortified Reliability and Robustness B-9
B.10 Vigilant System Monitoring B-11
B.11 Convenient Task Management B-12
B.12 Extensive Supportive Tools B-13

B.13 Easy-To-Use User Interfaces B-14

Appendix C: Boot Utility

C.1 (N) Set IP address C-2
C.2 (L) Load Image by TFTP C-3
C.3 (B) Update Boot ROM C-4
C.4 (S) Update System ROM C-4
C.5 (H) Utility menu C-5
C.6 (P) Set password C-5
C.7 (R) Restart system C-5
C.8 (Q) Quit & Boot RAID system C-5

Appendix D: Event Log Messages

D.1 RAID D-1
D.2 Task D-8
D.3 Disk D-25
D.4 Host ports D-37
D.5 Controller hardware D-48
D.6 Enclosure D-51
D.7 System D-59
D.8 Network D-67
D.9 Miscellaneous D-68
D.10 Snapshot D-68

List of Tables

Table 2-1 Buttons in monitor and config mode 2-6
Table 2-2 Hard disk code 2-6
Table 2-4 Information icons 2-7
Table 2-3 Hard disks tray color 2-7
Table 2-5 Components at the rear side of the system 2-10
Table 2-6 Login usernames and passwords 2-11
Table 2-7 Supported number of redundant SAS JBOD chassis and hard disks 2-12
Table 2-8 Information icons (in SAS monitor mode) 2-17
Table 2-9 Performance profile values 2-19
Table 2-10 Hard disk information 2-21
Table 2-11 Limitations of the number of member disks 2-44
Table 2-12 State transition 2-53
Table 3-1 List of status messages 3-3
Table 3-2 List of emergent messages 3-4
Table 3-3 List of background task messages 3-5
Table 5-1 MPIO device information 5-10
Table 5-2 System status information 5-69
Table 6-1 The capacity correlated with sector size 6-9

List of Figures

Figure 1-1 Layered storage objects 1-8
Figure 2-1 GUI login screen 2-1
Figure 2-2 Setting the language in Firefox 2-2
Figure 2-3 Languages dialog (Firefox) 2-3
Figure 2-4 Multiple system viewer (side button) 2-3
Figure 2-5 Opening the multiple system viewer 2-4
Figure 2-6 Single controller GUI monitor mode 2-5
Figure 2-7 Redundant-controller system GUI monitor monitor mode 2-5
Figure 2-8 HDD Tray (GUI) 2-6
Figure 2-9 Rear side of the RAID system (GUI) 2-9
Figure 2-10 Rear side of the redundant fiber RAID system (A16R-FS) 2-10
Figure 2-11 Rear side of the redundant SAS RAID system (A16R-SS) 2-10
Figure 2-12 Login section 2-11
Figure 2-13 Rear side of the SAS JBOD chassis (GUI) 2-13
Figure 2-14 Single SAS JBOD connection 2-14
Figure 2-15 Redundant SAS JBOD (A16R-SJ) loop connection 2-15
Figure 2-16 SAS enclosure monitor mode 2-16
Figure 2-17 SAS enclosure configuration mode 2-16
Figure 2-18 Overview screen 2-18
Figure 2-19 Method switching message 2-36
Figure 2-20 Simple storage 2-37
Figure 2-21 Symmetric storage 2-38
Figure 2-22 Selective storage 2-40
Figure 2-23 Specify the percentage for Bad Block Alert 2-58
Figure 2-24 Specify the percentage for Bad Block Clone 2-58
Figure 2-25 Event log download message 2-65
Figure 2-26 Options in the Configurations screen-1 (System Management menu) 2-68
Figure 2-27 Options in the Configurations screen-2 (System Management menu) 2-69
Figure 2-28 Options in the Configurations screen-3 (System Management menu) 2-69
Figure 2-29 Options in the Configurations screen-4 (System Management menu) 2-70
Figure 3-1 LCD manipulation procedure 3-1

Figure 3-2 Menu tree 3-6
Figure 4-1 Interfaces to Access CLI 4-1
Figure 5-1 Dual independent MPIO hosts 5-4
Figure 5-2 Clustered server environment 5-6
Figure 5-3 Computer Management screen: Device Manager 5-9
Figure 5-4 MPIO device screen 5-10
Figure 5-5 MTID environment 5-19
Figure 5-6 Redundant Single MPIO host (dual channel) 5-25
Figure 5-7 Redundant Single MPIO host (quad channel) 5-27
Figure 5-8 Redundant Dual Independent MPIO hosts 5-29
Figure 5-9 Dual clustering MPIO hosts 5-31
Figure 5-10 Active-Passive Redundant Single MPIO host 5-33
Figure 5-11 Controller failover scenario 5-35
Figure 5-12 Controller failover scenario 5-36
Figure 5-13 Controller failover and the page redirection message 5-37
Figure 5-14 Controller failback message 5-37
Figure 5-15 Error message indicates both controller failures 5-37
Figure 5-16 Relationship of volumes 5-40
Figure 5-17 SAN Environment 5-46
Figure 5-18 Defragment a disk group to expand the last free chunk 5-51
Figure 5-19 Defragment a disk group to consolidate free chunks 5-51
Figure 5-20 Logical disk capacity shrink and expanding an adjacent free chunk 5-52
Figure 5-21 Logical disk capacity shrink and creating a new free chunk 5-52
Figure 5-22 Logical disk capacity expansion by allocating an adjacent free chunk 5-52
Figure 5-23 Logical disk capacity expansion by moving logical disks to a free chunk 5-53
Figure 5-24 Logical disk capacity expansion by allocating an adjacent free chunk and moving logical disks 5-53
Figure 5-25 Disk group expansion by adding new member disks and enlarging the last free chunk 5-54
Figure 5-26 Disk group expansion by adding new member disks and creating a new free chunk 5-54
Figure 5-27 Disk group expansion to consolidate free chunks 5-54
Figure 5-28 Striping member volumes 5-55
Figure 5-29 Concatenating member volumes 5-55
Figure 5-30 Concatenated striping member volumes 5-55

Figure 5-31 Deployment example of RAIDGuard Central components 5-60
Figure 5-32 RGC Server monitor screen 5-63
Figure 5-33 RGC Agent monitor screen 5-64
Figure 5-34 RGC GUI main screen 5-65
Figure 5-35 Adding the IP address of an agent 5-67
Figure 5-36 Scanning the online RAID systems in the specified IP range 5-68
Figure 5-37 Scanning the online RAID systems in the selected agent's domain .5-68
Figure 5-38 Registering a RAID system to an agent 5-70
Figure 5-39 RGC GUI - System Panel 5-71
Figure 5-40 VDS Provider illustration 5-73
Figure 5-41 VDS Provider Configure screen 5-75
Figure A-1 RAID 0 disk array A-3
Figure A-2 RAID 1 disk array A-4
Figure A-3 RAID 3 disk array A-5
Figure A-4 RAID 5 disk array A-6
Figure A-5 RAID 6 disk array A-7
Figure A-6 RAID 10 disk array A-8
Figure A-7 RAID 30 disk array A-9
Figure A-8 RAID 50 disk array A-10
Figure A-9 RAID 60 disk array A-11
Figure A-10 JBOD disk array A-12
Figure A-11 NRAID A-13

Revision History

Version	Description	Release Date
1.0	Initial release	2006/09/22
1.01	2.2.2 Added detailed information of information icons shown in Monitor Mode. 2.2.3 Added detailed information of components shown in Monitor Mode. 2.4.2 Removed the restrictions on the number of spare disks for quick setup. 2.5.1 Added a note for the Disk Cache field shown in [RAID Management] > [Hard Disks]. 2.6.1/ 2.6.2/ 2.6.3/ 2.6.4/ 2.6.6 Modified the contents for the Schedule option. 2.6.8 Added the contents for the Schedule option. 2.7.1 Added a caution for the boot-up delay time. 2.9.2 Added a note for the NVRAM configuration. 2.9.3 Modified the descriptions for the DHCP method. Added the Authentication option for the SMTP server configuration. Appendix C Updated event log messages.	2007/01/24
1.1	• Changed all name lengths from characters to bytes. • Modified the descriptions for the 'Force to delete LUN mapping(s)' option. • Changed 'RAID array' to 'array'. 1.1 Updated key features. 1.3 Modify volume definition, add SSL definition. 2.1.1 Added browser language setting. 2.1.2 Added multiple system viewer. 2.2.1 Updated Figure 2-5. 2.3 Added SAS enclosure display.	2007/02/26

Version	Description	Release Date
1.1	2.4 Added Figure 2-10 (Overview screen) and modified the related descriptions. 2.5.2 Modified the hard disk state for quick setup. 2.6.1 Added one category, mode, and its definition. Added a note for the Modify button. 2.6.4 Added options to LD read algorithm. 2.6.6 Updated the Figure 2-11. 2.7.5 Modified the note for LD shrink. 2.7.6 Added expanding volumes. 2.7.7 Added shrinking volumes. 2.7.11 Added the contents for the Schedule option. 2.7.13 Added a note for the Force to recover disk option. 2.7.14 Add DST to the scheduled task. 2.7.15 Added spare restore control and task notify. 2.8.1 Added disk standby mode, added the range for the Delay Time When Boot-Up option. 2.8.2 Added the connection mode displayed on the FC ports page, added the configuration steps. 2.9.1 Added modify event receivers. 2.9.2 Added modify SNMP servers. 2.9.3 Added descriptions for the event log file. 2.10.1 Modified the hard disk states for the 'Erase configurations on HDD(s)' option. 2.10.2 Updated the Figure 2-18, 2-19, 2-20, and 2-21 and modified the related descriptions. 2.10.5 Added SSL setting. 2.10.7 Modified battery information. 2.10.9 Added descriptions for the regular system shutdown procedure. 2.10.10 Added Miscellaneous. Move the 'GUI refresh rate' option to this section.	2007/02/26

Version	Description	Release Date
1.1	2.11 Modified the descriptions related to the Reset button. 2.11.4 Added a note to explain the displayed information in the list. 3.2.3 Added UPS off emergent info. 3.2.5 Added hotkeys. Chapter 4 Updated CLI commands. Appendix C Updated event log messages.	2007/02/26
1.2	1.3 Modified descriptions related to the logical disk expansion and logical disk shrink. 2.2.2 Modified descriptions related to the information icons. 2.2.3 Modified the descriptions related to the rear side of the RAID system and picture, include added SAS controller picture. added component of Table 2-5. 2.6.1 Added descriptions related to the disk identify option of Modify. 2.6.6 Modified descriptions related to the WWN setting, added a SAS Address setting for symmetric and selective method. 2.9.4 Added support smart-UPS info. 2.10.8 Modified descriptions related to the external enclosure F/W. 2.10.10 Add memory testing when boot-up option in Miscellaneous. 2.11 Removed screen 2-22,2-22,2-23,2-24. 3.2.1 Modified disk status. 3.2.5 Added a ESC button function of Hotkeys. 4.1 Added descriptions for SSH info. Appendix D Added PathGuard MPIO Utility. Appendix E Added DiskPart Utility.	2007/07/15

Version	Description	Release Date
1.3	• Modified Company Address 2.2.3 Modified the descriptions related to the rear side of the RAID system and picture, include added SCSI controller picture. added component of Table 2-5. 2.6.6 Added a SCSI ID setting for simple method. 2.8.2 Added a Default SCSI ID setting for SCSI ports and provider setting data rate of SCSI on SCSI ports. Appendix F Added RAIDGuard Central. Appendix G Added VDS Provider.	2007/10/29
1.4	Chapter 1 Updated contents. 2.1.1 Added language setting in Firefox. 2.2.1 Updated the hard disk tray color. 2.2.3 Added the rear side of redundant-controller system. 2.3 Added the rear view and descriptions of the SAS JBOD chassis and its identifiers. 2.5 Added notes for the redundant-controller system and the different parameters in the degraded mode. 2.6.2 Added preferred controller option and VVOL button for JBOD disks. 2.6.4 Added preferred controller option and VVOL button for logical disks. 2.6.5 Added preferred controller option and VVOL button for volumes. 2.6.6 Added Virtual Volumes. 2.7.15 Added the new option 'Mirrored Write Cache Control' 2.8.2 Added a note for the FC port identifiers in the redundant-controller system, and descriptions for the WWNN button.	2008/02/25

Version	Description	Release Date
1.4	2.9.2 Added the new option 'Port' for the SNMP setting, and a note for the OIDs used for each SNMP version. 2.9.5 Added the new option 'Path Failover Alert Delay" and a new check item 'Controller Failure' for Auto Write-Through Cache option. 2.10.6/2.10.7/2.10.9/2.11.1/2.11.2/ 2.11.3 Added a note to for the screen difference in the redundant-controller system. Chapter 4 Updated CLI commands. Appendix B Added Features and Benefits. Appendix C Added screen and descriptions for the redundant-controller system. Appendix D Updated event log messages. Chapter 5 Modified Multi-path IO solution on 5.1. Added 5.2 Redundant Controller. Added 5.3 Snapshot Move all related advanced functions/ utilities from appendices to Chapter 5.	2008/02/25
1.4.1	Chapter 4 Updated CLI commands. Chapter 5 Modified Multi-path IO solution on 5.1.	2008/03/28

Version	Description	Release Date
1.4.2	Chapter 1 Added CLI In-band API Features. Added Snapshot function note. Chapter 4 Added support CLI In-band API. Modified 4.12 snapshot commands. Chapter 5 Added 5.1.8 Multi-path IO solution on SUN Solaris. Modified 5.3 Snapshot contents. Appendix D Modified D.10 snapshot events.	2008/05/05

Version	Description	Release Date
1.5	Chapter 6 Modified content of all. Chapter 5 Modified section 5.2. Move 5.2.2 Monitor Mode to 2.2. Move 5.2.2 SAS JBOD to 2.3. 2.9.2 Added SNMP agent functions. Added descriptions related SNMP MIB. 5.3.5 Removed. 5.3.6 Removed. 5.3.7 Removed. 2.6.6 Added descriptions related spare COW volumes functions. Added descriptions related Restore functions. Appendix C Revised the subtitles. 2.10.4 Added a Note. Chapter 1 Modified snapshot functions content. Modified system monitoring functions content. Modified management interfaces content. 1.4 Added Virtual disks descriptions. 1.5 Added SNMP Manager descriptions. Appendix D Updated snapshot events. Chapter 4 Updated CLI commands. 2.7.15 Added a Note of mirrored write cache. 2.1 Added browser support.	2008/07/03

Version	Description	Release Date
1.6	Chapter 5 Modified section 5.2. Inserted Multiple ID solutions in section 5.2 2.2.3 Modified redundant controller RAID pictures 2.3.1 Modified redundant controller RAID pictures. Added RAID model names 2.8.2 Modified description. Added Controller Failover mode description.	2008/11/14

Chapter 1: Introduction

Congratulations on your purchase of our RAID controller. Aiming at serving versatile applications, the RAID controller ensures not only data reliability but also improves system availability. Supported with cutting-edge IO processing technologies, the RAID controller delivers outstanding performance and helps to build dependable systems for heavy-duty computing, workgroup file sharing, service-oriented enterprise applications, online transaction processing, uncompressed video editing, or digital content provisioning. With its advanced storage management capabilities, the RAID controller is an excellent choice for both on-line and near-line storage applications. The following sections in this chapter will present an overview of features of the RAID controller, and for more information about its features and benefits, please see Appendix B.

1.1 Overview

- **Seasoned Reliability**

  The RAID controller supports various RAID levels, 0, 1, 3, 5, 6, and including multi-level RAID, like RAID 10, 30, 50, and 60, which perfectly balances performance and reliability. To further ensure the long-term data integrity, the controller provides extensive maintenance utilities, like periodic SMART monitoring, disk cloning, and disk scrubbing to proactively prevent performance degradation or data loss due to disk failure or latent bad sectors.

  The controller also supports multi-path I/O (MPIO) solutions tolerating path failure and providing load balance among multiple host connections for higher availability and performance. Together with active-active redundant-controller configuration, the RAID system offers high availability without single point of failure.

- **Great Flexibility and Scalability**

  Nowadays, IT staff is required to make the most from the equipments purchased, and thus easier sharing and better flexibility is a must for business-class storage systems. The RAID controller allows different RAID configurations, like RAID levels, stripe sizes, and caching policies, to be deployed independently for different logical units on single disk group, such that the storage resources can be utilized efficiently by fulfilling different requirements.

  As business grows or changes during the lifetime of storage systems, the requirements are very likely to be changed, and the users need to reconfigure the system to support the business dynamics while maintaining normal operations. The RAID controller allows capacity expansion by adding more disk drives or expansion chassis.

Comprehensive online reconfiguration utilities are available for migration of RAID level and stripe size, volume management, capacity resizing, and free space management.

- **Outstanding Performance**

  The RAID controller delivers outstanding performance for both transaction-oriented and bandwidth-hungry applications. Its superscalar CPU architecture with L2 cache enables efficient IO command processing, while its low-latency system bus streamlines large-block data transfer.

  In addition to the elaborated RAID algorithms, the controller implements also sophisticated buffer caching and IO scheduling intelligence. Extensive IO statistics are provided for monitoring the performance and utilization of storage devices. Users can online adjust the optimization policy of each LUN based on the statistics to unleash the most power of the controller.

- **Comprehensive and Effortless Management**

  Users can choose to manage the RAID systems from a variety of user interfaces, including command line interface over local console and secure shell (SSH), LCD panel, and web-based graphical user interface (GUI). Events are recorded on the NVRAM, and mail is sent out to notify the users without installing any software or agents. Maintenance tasks like capacity resizing and disk scrubbing are online executable, and can be scheduled or periodically executed. With the comprehensive management utilities, users can quickly complete the configurations and perform reconfiguration effortlessly.

1.2 Key Features

- **Basic RAID Construction**
  - Multiple RAID levels: 0, 1, 3, 5, 6, 10, 30, 50, 60, JBOD, and NRAID
  - Multiple stripe sizes (KB): 4, 8, 16, 32, 64, 128, 256, and 512.
  - Independently-selectable strip size for each logical disk
  - Independently-selectable RAID level for each logical disk
  - Support Quick Setup for effortless and quick RAID configuration
  - Support hot spare with global spare and local spare
  - Support auto spare and spare restore options
  - Support auto online disk rebuilding and configurable rebuild modes
  - Multiple disk rebuilding modes: parallel, sequential, and prioritized
  - Support up to 8 disk groups and 32 logical disks per disk group

- Support up to 24 disks in one chassis and totally 64 drives with expansion units

- **Volume management**
  - Support striping volume for performance enhancement
  - Support concatenating volume for large-capacity LUN
  - Support concatenated striping volume
  - Online volume capacity expansion
  - Online volume capacity shrink
  - Support up to 32 volumes and 8 logical disks per volume

- **Augmented RAID Features**
  - Flexible free chunk management
  - Multiple RAID initializations: none, regular (write-zero), and background
  - Support disk group write-zero initialization
  - Support user-configurable disk group capacity truncation
  - Support alignment offset
  - Support intelligent computation for RAID data and parity
  - Support fast read I/O response
  - Support NVRAM-based write log and auto parity consistency recovery
  - Support online bad block recovery and reallocation
  - Support battery backup module (BBM) for data retention during no power

- **Caching and Performance Optimizations**
  - Selective cache unit sizes (KB): 4, 8, 16, 32, 64, and 128
  - Independently-selectable caching policies for each LUN
  - Selective pre-read options with pre-read depth
  - Adaptive pre-read algorithms for sequential read workload
  - Selective write caching policies: write-through and write-behind (delay write)
  - Selective cache flush period with manual flush utility
  - Support intelligent write I/O merging and sorting algorithms
  - Support intelligent disk I/O scheduling
  - Selective performance profile: AV streaming, Max IOPS, and Max throughput

- **RAID Reconfiguration Utilities**
  - Online disk group expansion
  - Online RAID level migration
  - Online stripe size migration
  - Online simultaneous execution of the operations above
  - Online disk group defragmentation for free space consolidation
  - Online simultaneous disk group expansion and defragmentation
  - Online logical disk capacity expansion
  - Online logical disk capacity shrink
  - Support rebuild-first policy for early recovery from RAID degradation
- **Data Integrity Maintenance Utilities**
  - Online logical disk parity regeneration
  - Online disk scrubbing (a.k.a. media scan or patrol read)
  - Online parity check and recovery
  - Online disk cloning and replacement, with automatic resuming cloning
  - Support skipping cloned sectors when rebuilding partially cloned disks
- **Background Task Management**
  - Background task progress monitoring
  - Support one-time or periodic scheduling of maintenance tasks
  - Support priority control for different types of background tasks, like rebuilding
  - Support manual abort background tasks
  - Support background task roaming
  - Support automatic resuming tasks when the system restarts
  - Support early notification of task completion
- **Array Roaming and Recovery**
  - Support Configuration on disk (COD) with unique ID for each disk drive
  - Support drive traveling
  - Support online and offline array roaming
  - Support automatic and manual roaming conflict resolution
  - Online array recovery for logical disks, disk groups, and volumes
- **Storage Presentation**

- Support multiple storage presentations: simple, symmetric, and selective
- Support dynamic LUN masking
- Independently-selectable access control for each host and LUN
- Independently-selectable CHS geometry and sector size for each LUN
- Support host grouping management
- Support up to 32 hosts, 16 host groups, and 32 storage groups
- Support up 1024 LUNs and 128 LUNs per storage group

- **Hard Disk Management**
  - Support hard disk adding and removal emulation utility
  - Support disk self test (DST) and disk health monitoring by SMART
  - Support SMART warning-triggered disk cloning
  - Support bad block over-threshold triggered disk cloning
  - Support disk cache control
  - Support disk auto standby when idle
  - Support disk and disk group visual identification by LED
  - Support disk sequential power-on
  - Extensive disk I/O parameters selective for different environments
- **Expansion Port Functions (model-dependent)**
  - Support SAS JBOD expansion units
  - Support SAS SMP and SAS STP protocols
  - Support external enclosure monitoring by SES
  - Selective external enclosure and disk polling period
- **Host Interface Functions (model-dependent)**
  - Support 4Gb/s Fibre Channel host interfaces (FC-SAS/SATA controller)
  - Support 3Gb SAS host interfaces (SAS-SAS controller)
  - Support Ultra320 SCSI host interfaces (SCSI-SATA controller)
  - Support T11 SM-HBA attributes statistics
  - Support multiple-path IO (MPIO) solutions
- **Management Interfaces**
  - Local management via RS-232 port and LCD panel
  - Remote management via Ethernet and TCP/IP
  - Support network address settings by static, DHCP, and APIPA

- Support web-based GUI via embedded web server (HTTP)
- Support multiple languages and on-line help on web GUI
- Web-based multiple RAID system viewer with auto system discovery
- Embedded Command Line Interface (CLI) via RS232 port, SSH, and telnet
- Host-side Command Line Interface (CLI) via FC/SAS/SCSI and TCP/IP
- Support in-band and out-of-band RAID management
- Support SSL for protecting management sessions over Internet
- Support RAIDGuard™ Central for remote centralized management

- **System Monitoring Functions**
  - Support monitoring and control of hardware components and chassis units
  - Support SMART UPS monitoring and alert over RS232 port
  - NVRAM-based event logging with severity level
  - Event notification via beeper, email (SMTP), and SNMP trap (v1 and V2c)
  - Selective event logging and notification by severity level
  - Support redundant multiple email server and SNMP agents
  - Support multiple event recipients of email and SNMP trap
  - Support SNMP GET commands for monitoring via SNMP manager
- **Redundant Controller Functions (model-dependent)**
  - Support dual active-active controller configuration
  - Online seamless controller failover and failback
  - Cache data mirroring with on/off control option
  - Auto background task transfer during controller failover and failback
  - Support simultaneous access to single disk drive by two controllers
  - Online manual transfer preferred controller of a virtual disk
  - Uninterrupted system firmware upgrade
- **Snapshot Functions (model-dependent)**
  - Support copy-on-write compact snapshot
  - Instant online copy image creation and export
  - Instant online data restore/rollback from snapshot
  - Support multiple active snapshots for single LUN

- Support read/writable snapshot
- Support spare volume for overflow
- Support online snapshot volume expansion
- Support snapshot configuration roaming

- **Miscellaneous Supporting Functions**
  - Support configurations download and restore
  - Support configurations saving to disks and restore
  - Support password-based multi-level administration access control
  - Support password reminding email
  - Time management by RTC and Network Time Protocol (NTP) with DST
  - Support controller firmware upgrade (boot code and system code)
  - Support dual flash chips for protecting and recovering system code
  - Support object naming and creation-time logging

NOTE

The features may differ for different RAID system models and firmware version. You may need to contact your RAID system supplier to get the updates.

1.3 How to Use This Manual

This manual is organized into the following chapters:

- **Chapter 1 (Introduction)** provides a feature overview of the RAID system, and some basic guidelines for managing the RAID system.
- **Chapter 2 (Using the RAID GUI)** describes how to use the embedded GUI for monitoring and configurations with information helping you to understand and utilize the features.
- **Chapter 3 (Using the LCD Console)** presents the operations of LCD console, which helps you to quickly get summarized status of the RAID system and complete RAID setup using pre-defined configurations.
- **Chapter 4 (Using the CLI Commands)** tabulates all the CLI commands without much explanation. Because there is no difference in functions or definitions of parameters between GUI and CLI, you can study the GUI chapter to know how a CLI command works.
- **Chapter 5 (Advanced Functions)** provides in-depth information about the advanced functions of the RAID system to enrich your knowledge and elaborate your management tasks.
- **Chapter 6 (TroubleShooting)** provides extensive information about how you can help yourself when encoutering any troubles.

• **Appendices** describe supporting information for your references.

If you are an experienced user, you may quickly go through the key features to know the capabilities of the RAID system, and then read only the chapters for the user interfaces you need. Because this RAID system is designed to follow the commonly-seen conventions in the industry, you will feel comfortable when dealing with the setup and maintenance tasks. However, there are unique features offered only by the RAID system, and the RAID systems may be shipped with new features. Fully understanding these features will help you do a better job.

If you are not familiar with RAID systems, you are advised to read all the chapters to know not only how to use this RAID system but also useful information about the technologies and best practices. A better starting point for your management tasks is to get familiar with the GUI because of its online help and structured menu and web pages. You also need to know the LCD console because it is the best way for you to have a quick view of the system's health conditions. If you live in an UNIX world, you probably like to use the CLI to get things done more quickly.

To avoid having an ill-configured RAID system, please pay attentions to the warning messages and tips in the manual and the GUI. If you find mismatch between the manual and your RAID system, or if you are unsure of anything, please contact your suppliers.

1.4 RAID Structure Overview

The storage resources are managed as storage objects in a hierarchical structure. The hard disks, the only physical storage objects in the structure, are the essence of all other storage objects. A hard disk can be a JBOD disk, a data disk of a disk group, or a local spare disk of a disk group. It can also be an unused disk or a global spare disk. The capacity of a disk group is partitioned to form logical disks with different RAID configurations, and multiple logical disks can be put together to create volumes using striping, concatenation, or both. The JBOD disks, logical disks, and volumes, are virtual disks, which can be exported to host interfaces as SCSI logical units (LUN) and serve I/O access from the host systems. Below are more descriptions about each storage objects.

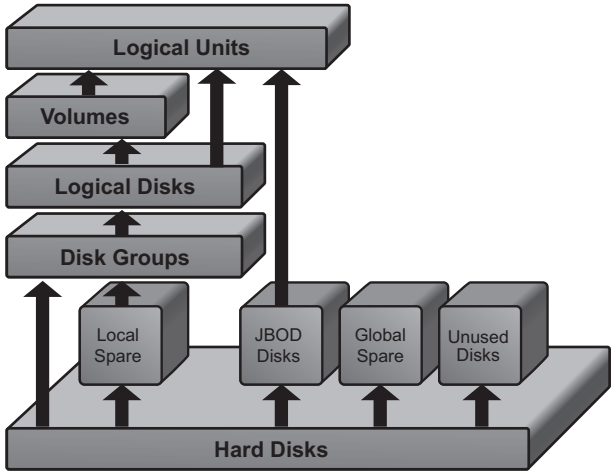


Figure 1-1 Layered storage objects

- **JBOD disk**

A JBOD (Just a Bunch Of Disks) disk is formed by single hard disk that can be accessed by hosts as a LUN exported by the controller. The access to

the LUN is directly forwarded to the hard disk without any address translation. It is often also named as pass-through disk.

- **Member disk**

  The hard disks in a disk group are member disks (MD). A member disk of a disk group can be a data disk or a local spare disk. A data member disk provides storage space to form logical disks in a disk group.

- **Disk group**

  A disk group (DG) is a group of hard disks, on which logical disks can be created. Operations to a disk group are applied to all hard disks in the disk group.

- **Logical disk**

  A logical disk (LD) is formed by partitioning the space of a disk group. Logical disks always use contiguous space, and the space of a logical disk is evenly distributed across all member disks of the disk group. A logical disk can be exported to hosts as a LUN or to form volumes.

- **Local spare and global spare disk**

  A spare disk is a hard disk that will automatically replace a failed disk and rebuild data of the failed disk. A local spare disk is dedicated to single disk group, and a global spare disk is used for all disk groups. When a disk in a disk group fails, the controller will try to use local spare disks first, and then global spare disks if no local spare is available.

- **Volume**

  A volume is formed by combining multiple logical disks using striping (RAID0) and concatenation (NRAID) algorithms. Multiple logical disks form single volume unit using striping, and multiple volume units are aggregated to form a volume using concatenation. A volume can be exported to hosts as a LUN.

- **Logical unit**

  A logical unit (LUN) is a logical entity within a SCSI target that receives and executes I/O commands from SCSI initiators (hosts). SCSI I/O commands are sent to a target device and executed by a LUN within the target.

- **Virtual disk**

  A virtual disk is an storage entity that can service I/O access from LUNs or from other virtual disks. It could be JBOD disk, logical disk, or volume. If a virtual disk is part of other virtual disk, then it cannot be exported to LUNs.

- **LUN mapping**

  A LUN mapping is a set of mapping relationships between LUNs and virtual disks in the controller. Computer systems can access the LUNs presented by the controller after inquiring host ports of the controller.

1.5 User Interfaces to Manage the RAID System

A variety of user interfaces and utilities are offered for managing the RAID systems, and you may choose to use one or multiple of them that suit your management purposes. Introduction to these interfaces and utilities is described as below:

- **Web-based GUI (chapter 2)**

  Web-based GUI is accessed by web browsers after proper setup of the network interfaces. It offers an at-a-glance monitoring web page and full-function system management capability in structured web pages. It is advised to use the web-based GUI to fully unleash the power of RAID system if you are a first-time user.

- **SNMP Manager (section 2.9.2 Setting up the SNMP)**

  SNMP (Simple Network Management Protocol) is a widely used protocol based on TCP/IP for monitoring the health of network-attached equipments. The RAID controller is equipped with an embedded SNMP Agent to support SNMP-based monitoring. You can use SNMP applications (SNMP v1 or v2c-compliant) at remote computers to get event notification by SNMP traps and watch the status of a RAID system.

- **LCD Console (chapter 3)**

  LCD console is offered for quick configuration and for display of simplified information and alerting messages. It is mostly for initializing network setting to bring up the web-based GUI or for knowing the chassis status. Using the LCD console for configuration is only advised when you know clearly the preset configurations.

- **CLI Commands (chapter 4)**

  Command line interface can be accessed by RS-232 port, TELNET, or SSH. You can also use host-based CLI software to manage RAID systems by in-band (FC/SAS/SCSI) or out-of-band (Ethernet) interfaces. It helps you to complete configurations in a fast way since you can type in text commands with parameters quickly without the need to do browse and click. You may also use CLI scripts for repeating configurations when deploying many systems.

- **RAIDGuard Central (chapter 5)**

  RAIDGuard Central is a software suite that helps you to manage multiple RAID systems installed in multiple networks. It locates these systems by broadcasting and will be constantly monitoring them. It receives events

from the systems, and stores all the events to single database. It also provides event notification by MSN messages.

- **Microsoft VDS (chapter 5)**

  VDS is a standard of RAID management interface for Windows systems. The RAID system can be accessed by VDS-compliant software after you install the corresponding VDS provider to your systems. This helps you to manage RAID systems from different vendors using single software. But note because VDS is limited to general functions, you need to use Web GUI or CLI for some advanced functions of this RAID system.

1.6 Initially Configuring the RAID System

Properly configuring your RAID systems helps you to get the most out of your investments on the storage hardware and guarantee planned service level agreements. It also reduces your maintenance efforts and avoids potential problems that might cause data loss or discontinued operations. It is especially true for a powerful and flexible RAID system like the one you have now. This section provides some basic steps and guidelines for your reference. The initial configuration has the following tasks:

1. Understanding your users' needs and environments
2. Configuring the hardware settings and doing health check
3. Organizing and presenting the storage resources
4. Installing and launching bundled software (optionally)
5. Getting ready for future maintenance tasks

- **Understanding your users' needs and environments**

  The first step for procuring or deploying any equipment is to know the users' needs and environments, assuming you've already known much about your RAID systems. Users' needs include the capacity, performance, reliability, and sharing. The environment information includes the applications, operating systems (standalone or clustered), host systems, host adapters, switches, topologies (direct-attached or networked storage), disk drives (enterprise-class, near-line, or desktop) and management networks. Extra cares are needed if you are installing the RAID systems to an existed infrastructure under operations. Check your RAID system supplier to ensure good interoperability between the RAID system and the components in your environments. You will also need to know the potential changes in the future, like capacity growth rate or adding host systems, such that you can have plans for data migration and reconfigurations. The quality of your configurations will largely depend on the information you collect. It is advised to write down the information of users' needs and environments as well as the configurations in your mind, which can be very helpful guidance through the all the lifetime of the RAID systems.

- **Configuring the hardware settings and doing health check**

  After installing your RAID systems with necessary components, like hard disks and transceivers, to your environment, enabling the user interfaces is a prerequisite if you want to do anything useful to your RAID systems. The only user interface that you can use without any tools is the LCD console, by which the settings of the RS232 port and the management network interface can be done to allow you to use the GUI and CLI (see **3.3 Menu on page 3-6**).

  Now, do a quick health check by examining the GUI monitoring page to locate any mal-functioning components in the chassis or suspicious events (section 2.2). Follow the hardware manual to do troubleshooting, if needed, and contact your supplier if the problems still exist. Make sure the links of the host interfaces are up and all installed hard disks are detected. Since your hard disks will be the final data repository, largely influencing the overall performance and reliability, it is advised to use the embedded self-test utility and SMART functions to check the hard disks (see **2.8 Hardware Configurations on page 2-56**). A better approach would be to use benchmark or stress testing tools.

  You need also be sure that all the attached JBOD systems are detected and no abnormal event reported for the expansion port hardware (see **2.3 SAS JBOD Enclosure Display (for SAS expansion controller only) on page 2-12**). Sometimes, you will need to adjust the hardware parameters, under your supplier's advices, to avoid potential interoperability issues.

- **Organizing and presenting the storage resources**

  The most essential configuration tasks of a RAID system are to organize the hard disks using a variety of RAID settings and volume management functions, and eventually to present them to host systems as LUNs (LUN mapping). This is a process consisted of both top-down and bottom-up methodology. You see from high-level and logical perspectives of each host system to define the LUNs and their requirements. On the other hand, you will do configuration starting from the low-level and physical objects, like grouping the disk drives into disk groups.

  Tradeoff analysis is required when choosing RAID levels, like using RAID 0 for good performance but losing reliability, or using RAID 6 for high reliability but incurring performance penalty and capacity overhead. The appendix provides information about the algorithms of each RAID level and the corresponding applications. You can also use the embedded volume management functions to build LUNs of higher performance and larger capacity. The RAID system offers much flexibility in configurations, like independently-configurable RAID attributes for each logical disk, such that capacity overhead can be minimized while performance and reliability can still be guaranteed.

  You might need to pay attentions to a few options when doing the tasks above, like initialization modes, cache settings, alignment offset rebuilding mode, and etc. Please read the GUI chapter to know their

meanings and choose the most appropriate settings, because they are directly or indirectly related to how well the RAID system can perform (see **2.6 RAID Management on page 2-21** and **2.7.16 Miscellaneous on page 2-55**).

NOTE

When planning your storage resources, reserving space for snapshot operations is needed. Please check chapter 5 for information about the snapshot functions.

- Installing and launching bundled software (optionally)

The RAID system is equipped with host-side software providing solutions for multi-path I/O, VDS-compliant management, and centralized management console on multiple platforms. You can locate their sections in the chapter 5 and know their features and benefits, as well as how to do the installation and configuration. Contact your RAID system supplier to know the interoperability between the software and the system.

NOTE

Installing multi-path I/O driver is a must for redundant-controller systems to support controller failover/failback. Please check **Chapter 5: Advanced Functions** for more information about MPIO and redundant-controller solution.

- Getting ready for future maintenance tasks

The better you're prepared, the less your maintenance efforts would be. Below are the major settings you'll need for maintenance.

Event logging and notification

You can have peace only if you can always get timely notifications of incidents happening to your RAID systems, so completing the event notification settings is also a must-do. You might also need to set the policies for event logging and notifications (see **2.9 Event Management on page 2-61**).

Data integrity assurance

For better system reliability, you are advised to set policies for handling exceptions, like to start disk cloning when SMART warning is detected or too many bad sectors of a hard disk are discovered (see **2.8.1 Hard disks on page 2-56**), or to turn off write cache when something wrong happens (see **2.9.5 Miscellaneous on page 2-67**). You may also schedule periodic maintenance tasks to do disk scrubbing(see **2.7.9 Scrubbing on page 2-49**) for defected sectors recovery or to do disk self-tests (see **2.7.11 Performing disk self test on page 2-50**).

Miscellaneous settings

There are also minor settings that you might need to do, like checking UPS (see **2.9.4 UPS on page 2-66**), time setup (see **2.10.4 System Time on page 2-71**), changing password (strongly suggested) and etc.

Saving the configurations

If you've done all the configurations, please save the configurations to files (human-readable text file for your own reference and binary file for restoring the configurations if any disaster happens).

1.7 Maintaining the RAID System

Properly configuring RAID systems is a good starting point, but you need to do regular checking and reconfiguration to make sure your RAID systems are healthy and delivering the best throughout the lifetime.

- **Constantly monitoring RAID system health**

You can quickly get an overview of the RAID system health by accessing the monitoring page of the Web GUI (see **2.2 Monitor Mode on page 2-5**). You probably need to do so only when receiving event notification email or traps. All the events are described in the Appendix D, each of which has suggested actions for your reference. You need to watch the status of chassis components, like fans, power supply units, battery module, and controller module. You need also check the status of hard disks, and the I/O statistics (see **2.11 Performance Management on page 2-76**) to know the system loading level and distribution. A hard disk with long response time or lots of media errors reported could be in trouble.

- **Performing online maintenance utilities**

Comprehensive maintenance utilities are offered for ensuring the best condition and utilization of your RAID systems all through its lifetime. They include data integrity assurance, capacity resource reallocation, and RAID attributes migration.

Data integrity assurance

For data long-term integrity assurance and recovery, you may use disk scrubbing (see **2.7.9 Scrubbing on page 2-49**), disk cloning (see **2.7.8 Cloning hard disks on page 2-47**), DST (see **2.7.11 Performing disk self test on page 2-50**), and SMART (see s **2.8.1 Hard disks on page 2-56**). For how these can help you, please go to **Appendix B: Features and Benefits**.

Capacity resource reallocation

If you'd like to add more disks for capacity expansion, you can use disk group expansion (see **2.7.1 Expanding disk groups on page 2-43**). Resizing logical disks and volumes (**2.7.4 Expanding the capacity of**

logical disks in a disk group on page 2-45 to **2.7.6 Expanding volumes on page 2-46**) can also help you to transfer the unused capacity of a LUN to others that are desperate for more space without any impact to other LUNs. If unused space is scattered, you can use disk group defragmentation (see **2.7.2 Defragmenting disk groups on page 2-43**) to put them together.

RAID level and strip size migration

Changing RAID level of a logical disk (see **2.7.3 Changing RAID level / stripe size for logical disks on page 2-44**) will significantly affect the performance, reliability, and space utilization. For example, you may add one disk to a two-disk RAID 1 disk group and change its RAID level to RAID 5, such that you can have a three-disk RAID 5 disk group, offering usable space of two disks. On the other hand, changing stripe size affects only the performance, and you may do as many online experiments as possible to get the performance you want.

Schedule a task

You won't want the performance degradation during the execution of the online maintenance utilities, which very like need non-trivial amount of time. To avoid such impact, you're allowed to schedule a task execution to any time you want (see **2.7.14 Schedule task on page 2-54**), like during off-duty hours. You can get event notifications when the task is done (or unfortunately fails), or at a user-configurable percentage of the task progress (see **2.7.16 Miscellaneous on page 2-55**).

Chapter 2: Using the RAID GUI

2.1 Accessing the RAID GUI

1. Open a browser and enter the IP address in the address field. (The default IP address is 192.168.0.1. You can use the FW customization tool to set another IP address as the default.)

   The supported browsers are listed as below:

   - IE 6.x (Windows)
   - IE 7.x (Windows)
   - FireFox 1.x (Windows, Linux, and Mac)
   - Safari 1.x and 2.x (Mac)

2. The following webpage appears when the connection is made. To login, enter the username and password (see **2.2.4 Login on page 2-11**). You can then access the Config Mode.

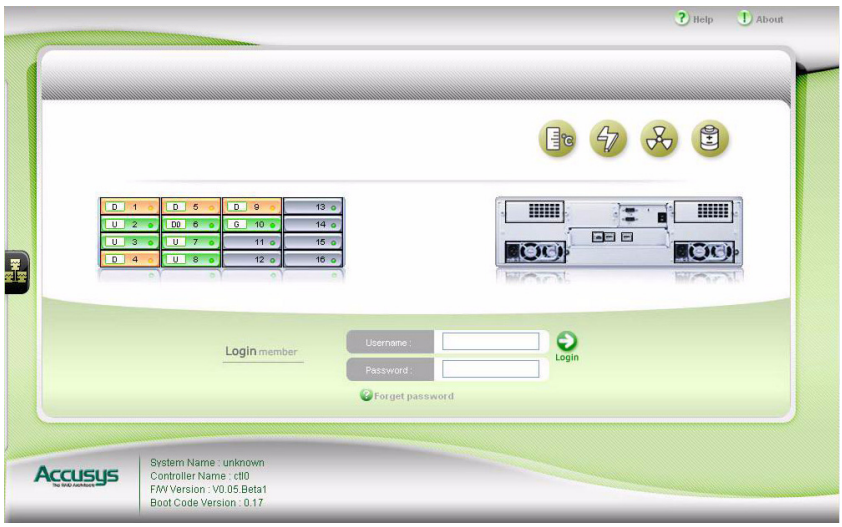


Figure 2-1 GUI login screen

2.1.1 Browser Language Setting

The GUI is currently available in English, Traditional Chinese, and Simplified Chinese. For other languages, you can use the FW customization tool to add multi-language support. (The following example shows how to set up language in Internet Explorer 6. Other browsers support the same functionality. Please refer to the instructions included with your browser and configure the language accordingly.)

Open your web browser and follow the steps below to change the GUI language.

1. Click **Tools > Internet Options > Language > Add**.

2. In the **Add Language** window, find the language you want to use, and click **OK**.
3. In the **Language Preference** window, select the language you want to use, and use the **Move Up** and **Move Down** buttons to move it up to the top of the list. Click **OK**.
4. Click **OK** again to confirm the settings.

NOTE

If the GUI does not support the selected language, the webpage will still appear in English.

- **Firefox language settings**

Here is an example of how to change the GUI language settings in Firefox.

1. Open the Firefox browser and select **Tools > Options > Advanced > General** tab.
2. Click the **Choose...** button to specify your preferred language for the GUI to display.

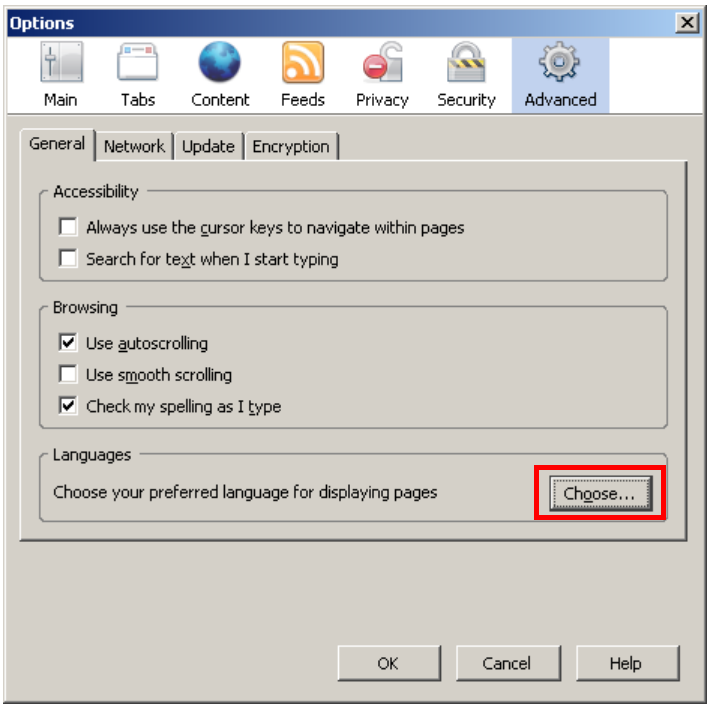


Figure 2-2 Setting the language in Firefox

3. The following Languages dialog displays. To add a language, click **Select a language to add...**, choose the language, and click the **Add** button. Use the **Move Up** and **Move Down** buttons to arrange the languages in order of priority, and the **Remove** button if you need to remove a language. Click **OK**.

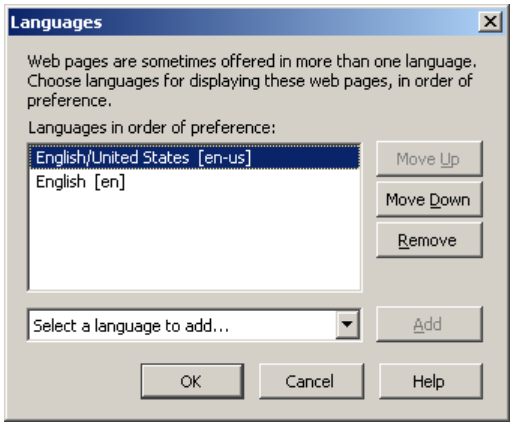


Figure 2-3 Languages dialog (Firefox)

4. Click **OK** again to confirm the settings.

2.1.2 Multiple System Viewer

The RAID GUI features a side button for a quick on-line system view. The side button is always on the left side of the screen so that you can click to view all the other on-line systems at anytime. Move the cursor over the side button and the multiple system viewer appears (see **Figure 2-5**).

Figure 2-4 Multiple system viewer (side button)

Figure 2-5 Opening the multiple system viewer

Move the cursor to a system, and the following system information will appear: IP address, System name, Model name, Firmware version, and Status. Click on a system to open its GUI, and you can login to view the complete system information.

If there are too many on-line systems displayed in the viewer at one time, you can use the arrow buttons to scroll up and down. Click the button to refresh the viewer.

Move your cursor away from the viewer, and it disappears.

NOTE

1. The multiple system viewer supports up to 256 on-line systems.
2. Only systems in the same subnet mask will appear in the multiple system viewer.

2.2 Monitor Mode

RAID GUI monitors the status of your RAID controller(s) through your Ethernet connection. The RAID GUI window first displays the Monitor Mode. This mode is also the login to enter Config Mode. The GUI components shown are introduced in the following sections.

Figure 2-6 Single controller GUI monitor mode

At the front view panel, there are 16 or 24 HDD trays displayed in the redundant-controller system. Depending on the redundant-controller system model, the number of HDDs may differ. Besides a maximum of eight enclosures can be connected to the subsystem serially while the single subsystem supports up to seven enclosures. For more information about the indications of HDD status code and color, see **2.2.1 HDD state on page 2-6**.

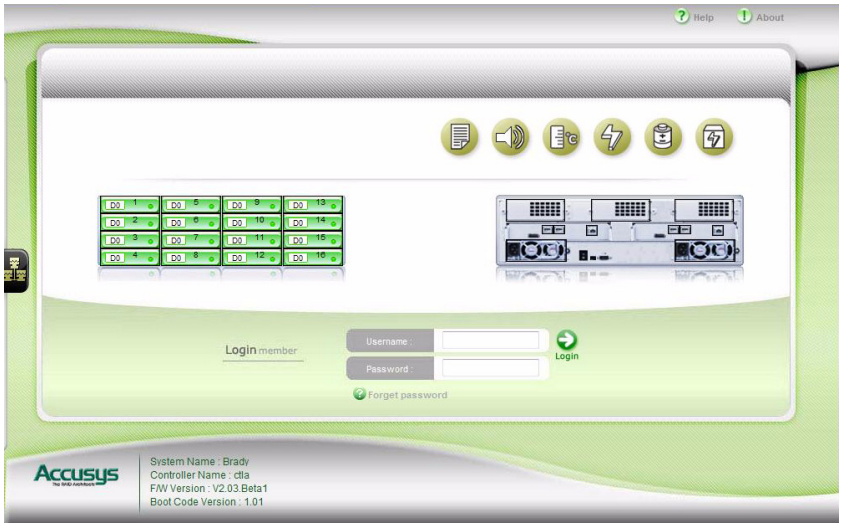


Figure 2-7 Redundant-controller system GUI monitor

There are four buttons at the top right of the page. See the following table for each button's function.

Button	Description
Switch Mode	Switches between Monitor Mode and Config Mode.
Logout	Logs out the user.
Help	Opens the Help file.
About	Displays the GUI version, firmware version, and boot code version.

Table 2-1 Buttons in monitor and config mode

System name, controller name, firmware version, and boot code version information are also displayed at the bottom left of the page.

2.2.1 HDD state

Through the front panel of the RAID console displayed in the GUI, you can easily identify the status of each hard disk by its color and status code. Click on each hard disk to display detailed information.

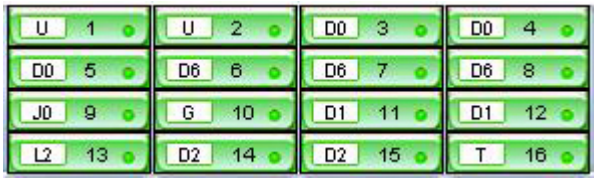


Figure 2-8 HDD Tray (GUI)

NOTE

The RAID system can support up to 24 HDD trays. The number of HDD trays displayed in the GUI monitor mode may differ depending on the RAID system model.

The status code and color of hard disks are explained in the following tables.

Code	Hard Disk Status
U	Unused disk
J0-J15	JBOD

Table 2-2 Hard disk code

Code	Hard Disk Status
D0-D7 D0-Dv	Disk group (The redundant-controller system supports up to 32 DGs, which are encoding from **D0** to **Dv**)
L0-L7	Local spare
G	Global spare
T	Clone

Table 2-2 Hard disk code

Color	Hard Disk Status	Color	Hard Disk Status
Green	Online Adding (flashing green)	Purple	Unknown
Red	Faulty	Silver	Permanently removed
Orange	Conflict	Gray	Removed
Blue	Foreign		Empty

Table 2-3 Hard disks tray color

2.2.2 Information icons

When components are working normally, their icons are shown in green. When components are uninstall, not norms or, failed, the icons are shown in red. Click on each icon for detailed information.

Icon	Name	Detailed Information
	Event log view	• Seq. No. • Severity • Type • Time • Description
	Beeper	See **6.2 Beeper on page 6-1** for the possible beeper reasons.
	Temperature	• Sensor • Current • Non-critical* • Critical*
	Voltage	• Sensor • Current • High Limit* • Low Limit*

Table 2-4 Information icons

	Fan module (This icon will be shown when the fan is installed on the controller.)	• Controller Fan
	BBM (This icon will be shown when the BBM control is on.)	• State • Remaining Capacity • Voltage (V) • Temperature (°C/°F) • Non-critical Temperature (°C/°F)* • Critical Temperature (°C/°F)*
	UPS (This icon will be shown when the UPS control is on.)	**UPS Status** • State • Load Percentage • Temperature (°C/°F) • AC Input Quality/ High Voltage (V)/ Low Voltage (V) **Battery Status** • State • Voltage (V) • Remaining Power in percentage/ seconds

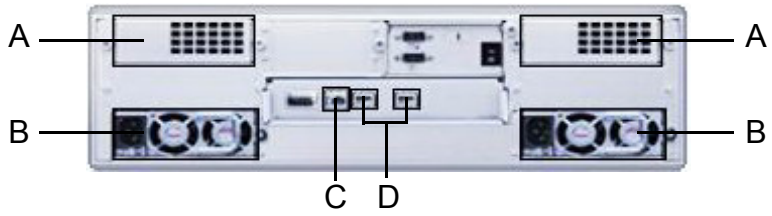
Table 2-4 Information icons

2.2.3 Rear side view

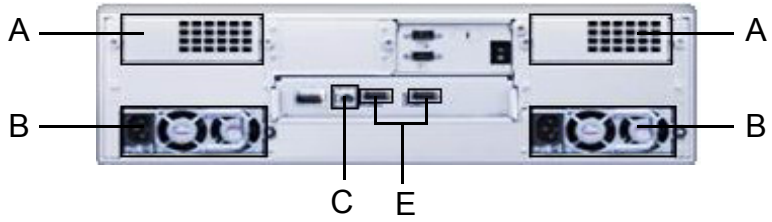
- For single-controller RAID system

On the rear side of the RAID system, you can see the fan modules, power supplies, two fiber ports (for fiber controller), two sas ports (for SAS controller), one Ethernet port, and SAS expansion port (for SAS expansion controller solution). Click on the components for detailed information.

Fiber Controller:



SAS Controller:



SCSI Controller:

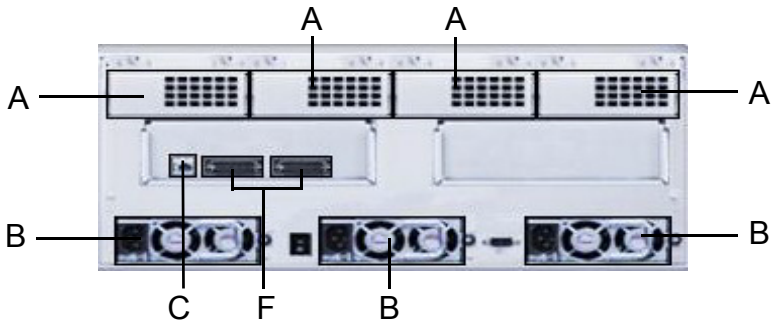


Figure 2-9 Rear side of the RAID system (GUI)

- For redundant-controller RAID system

Figure 2-10 illustrates the rear components at the rear of the redundant-controller system. Two controllers, controller A and controller B, are located from left to right as shown. Therefore, fiber ports on the controller A are fcpa1and fcpa2; fiber ports on the controller B are fcpb1and fcpb2.

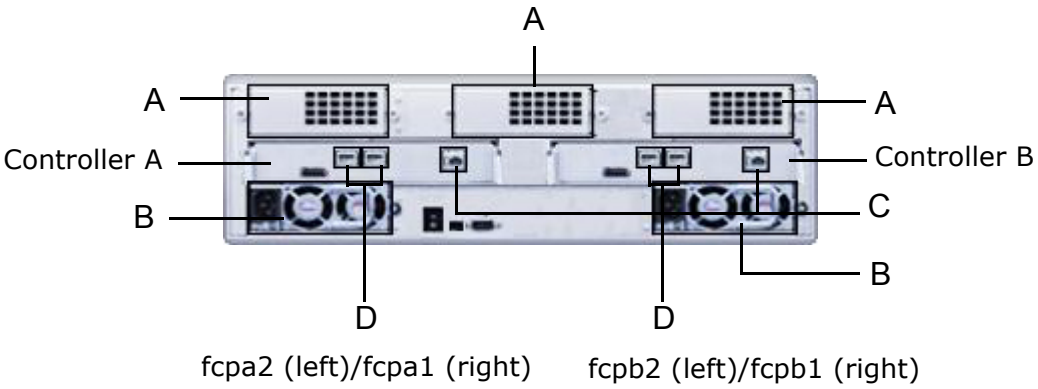


Figure 2-10 Rear side of the redundant fiber RAID system (A16R-FS

Instead of four fiber ports equipped with the redundant fiber controller. There are four SAS ports located on both controller A and B. See the port identifiers as shown in **Figure 2-11**.

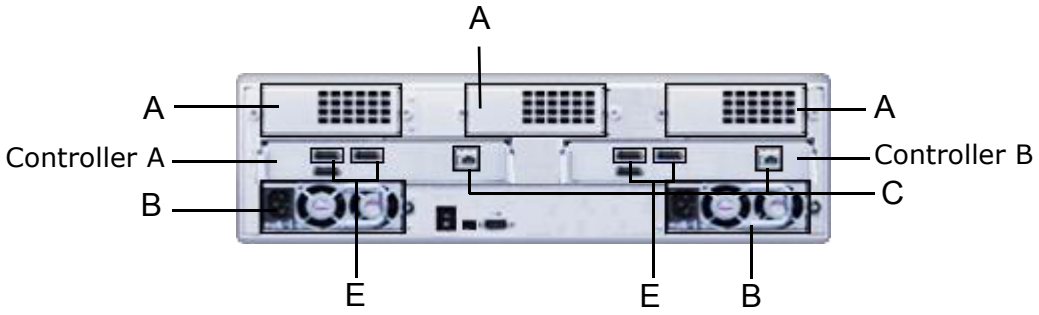


Figure 2-11 Rear side of the redundant SAS RAID system (A16R-SS)

	Component	Detailed Information
A	Fan module	• BP_FAN1 • BP_FAN2 • BP_FAN3 • BP_FAN4

Table 2-5 Components at the rear side of the system

B	Power supply	• POW1 • POW2 • POW3
C	Ethernet port	• IP Address • Network Mask • Gateway • DNS Server • MAC Address
D	Fiber ports	• FCP ID • WWN • Connection Mode • Date Rate • Hard Loop ID
E	SAS ports	• SAS ID • SAS Address
F	SCSI ports	• SCSI ID • Data Rate • Default SCSI ID

Table 2-5 Components at the rear side of the system

2.2.4 Login

Figure 2-12 Login

The RAID GUI provides two sets of default login members.

Username	user	admin
Password	0000	0000

Table 2-6 Login usernames and passwords

When logging in to the GUI as **user**, you can only view the settings. To modify the settings, use **admin** to log in.

- Forgotten password

In the event that you forget your password, click the **Forget password** icon and an email containing your password can be sent to a preset mail account. To enable this function, make sure the Password Reminding Mail

option is set to On (see **2.10.5 Security control on page 2-72**), and the mail server has been configured in **System Management > Network**.

NOTE

You can use the FW customization tool to set a new password as the default.

2.3 SAS JBOD Enclosure Display (for SAS expansion controller only)

The single controller RAID subsystem provides a SAS expansion port which allows users to connect a SAS JBOD.The single controller support 120 hard disks so a maximum of six enclosures can be connected to the subsystem serially, and each enclosure supports up to 16 SAS hard disks.

Each redundant-controller system provides two SAS expansion ports to connect with one or more SAS JBOD chassis. While the single SAS JBOD chassis only supports 16-bay RAID system, the redundant SAS JBOD chassis is designed in two models, 16-bay and 24-bay. Depending on the redundant-controller system and SAS JBOD chassis models (16-bay or 24-bay) as well as the memory size in use (1G or 2G), the GUI may have different enclosure tabs and front tray view displayed. See **Table 2-7** below for the supported number of SAS JBOD chassis and hard disks.

RAID Subsystem model	Memory size	Units of HDD	SAS JBOD (16-bay)	SAS JBOD (24-bay)
16-bay	1G	64	3	2
	2G or higher	120	7*	5*
24-bay	1G	64	3*	2*
	2G or higher	120	6	4

Table 2-7 Supported number of redundant SAS JBOD chassis and hard disks

* Please note that there are some empty slots shown in the SAS JBOD enclosure display (in the last enclosure tab) due to the maximum number of supported drives.

2.3.1 Rear side monitor of the SAS JBOD chassis

On the rear side of the SAS JBOD chassis, there are three ports (for single SAS JBOD) or six ports (for redundant SAS JBOD) available for SAS JBOB expansion. See the port identifiers as shown in **Figure 2-13**.

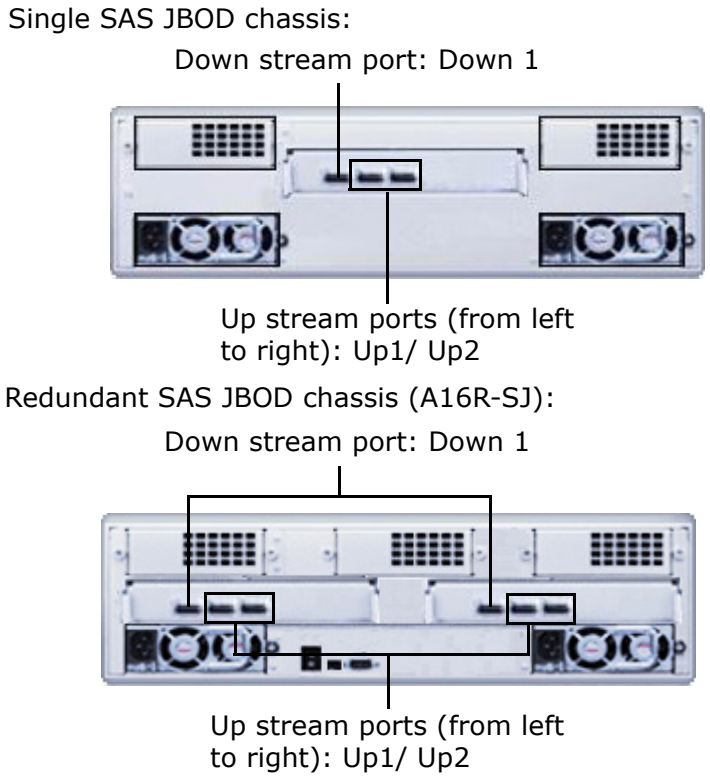

Single SAS JBOD chassis:
Down stream port: Down 1
Up stream ports (from left to right): Up1/ Up2
Redundant SAS JBOD chassis (A16R-SJ):
Down stream port: Down 1
Up stream ports (from left to right): Up1/ Up2

Figure 2-13 Rear side of the SAS JBOD chassis (GUI)

2.3.2 SAS JBOD Installation with RAID subsystem

- For single controller with single JBODs:

Use the down and up stream ports to connect the RAID subsystem with up to three SAS JBODs. **Figure 2-14** shows a serial construction for expanded JBOD disks. Connect the RAID subsystem's SAS port to the up stream port of a SAS JBOD using a Mini SAS cable. For more expanded JBOD chassis, connect the down stream port on the previously connected SAS JBOD to the up stream port on the other SAS JBOD.

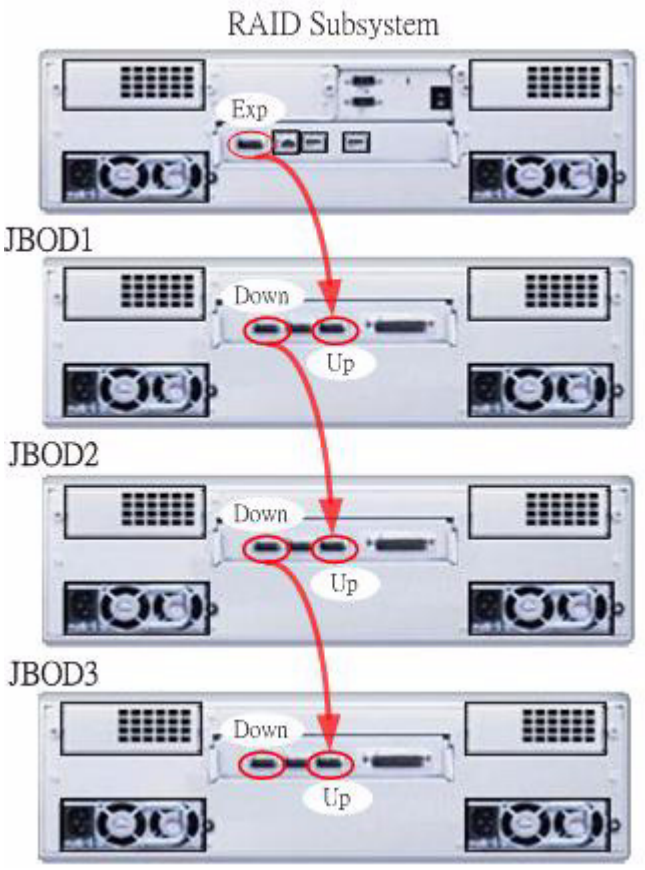


Figure 2-14 Single SAS JBOD connection

- **For redundant controller with redundant JBODs (A16R-SJ)**

  To ensure the system can continue its operation without any interruption in the event of any SAS JBOD failure, a loop construction is suggested. **Figure 2-15** shows an example of the loop implementation with a redundant RAID system and SAS JBODs. Users can create as below:

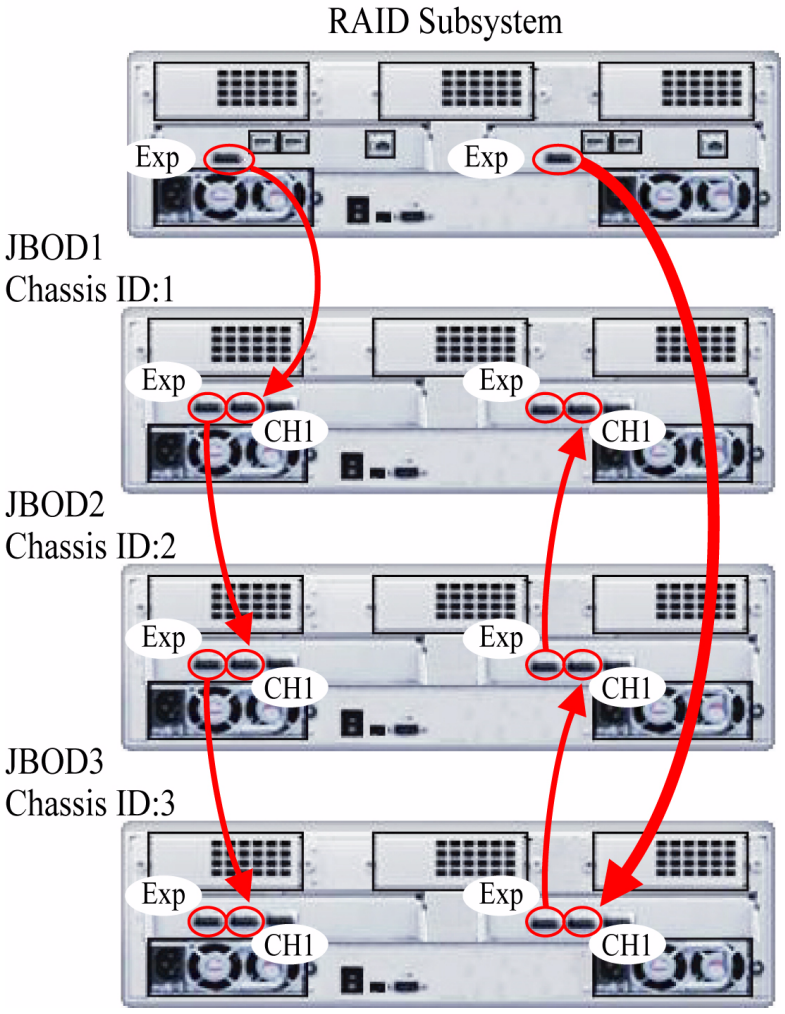


Figure 2-15 Redundant SAS JBOD (A16R-SJ) loop connection

The connection shown in **Figure 2-15** enables all the three JBOD chassis to be looped through the redundant-controller system. In this way, the data is transmitted from node to node around the loop. Once the JBOD2 is failed and causes interruption, JBOD1 and JBOD3 still work normally via the redundant path.

2.3.3 Monitor mode

When SAS JBOD chassis are connected, the enclosure tabs will appear in the Monitor Mode (see **Figure 2-16**). Each tab view displays different information for each connected enclosure. Click the **Enclosure 0** tab to view the information of the local RAID subsystem. Click the **Enclosure 1**, **Enclosure 2**, or **Enclosure 3** tabs for a brief view of the connected SAS JBOD.

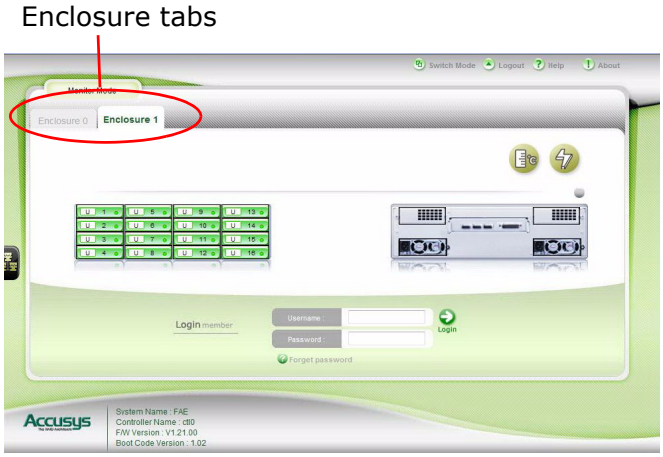


Figure 2-16 SAS enclosure monitor mode

Each SAS JBOD has an unique chassis identifier, which can be detected automatically by the GUI when connected. The chassis identifier corresponds to the enclosure tab number shown in the GUI. In this way, users can identify and manage each SAS JBOD easily and correctly. However, the enclosure tabs are always displayed in ascending order of chassis identifiers instead of the chassis connection order.

The number of enclosure tabs may be different according the number of connected SAS JBOD chassis. For more information, see • **For redundant controller with redundant JBODs (A16R-SJ)**.

Figure 2-17 displays the Config Mode when a SAS enclosure is connected. Use the drop-down menu at the top of the page to select the enclosure ID you wish to configure.

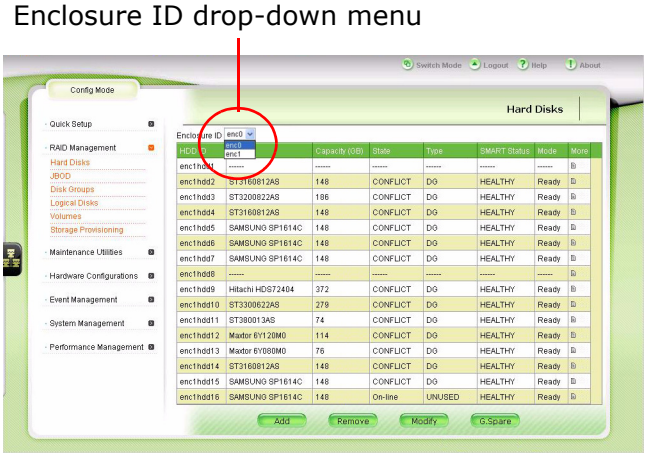


Figure 2-17 SAS enclosure configuration mode

NOTE

In order to use the expansion port on the SAS controller, you must have firmware version 1.20 or later for complete functionary.

2.3.4 Information icons

In Monitor Mode, the following information icons are displayed on the screen. When components are working normally, their icons are shown in green. When components fail to work, the icons are shown in red. Click on each icon for detailed information.

Icon	Name	Detailed Information
	Temperature	• Sensor • Current • Non-critical • Critical
	Voltage	• Sensor • Current • High Limit • Low Limit
	Fan module	• BP_FAN1 • BP_FAN2 • BP_FAN3 • BP_FAN4
	Power supply	• POW1 • POW2

Table 2-8 Information icons (in SAS monitor mode)

2.3.5 SAS/SATA HDD information

Through the hard disk codes and tray color shown on the screen, you can easily identify the status of each connected SAS/SATA hard disk. Click on each SAS/SATA hard disk to display detailed information.

For more information about hard disk codes and tray colors, see **Table 2-2** and **Table 2-3 on page 2-7**.

2.4 Config Mode

To configure any settings under Config Mode, log in with ***admin*** and its password. The **Overview** screen displays as below.

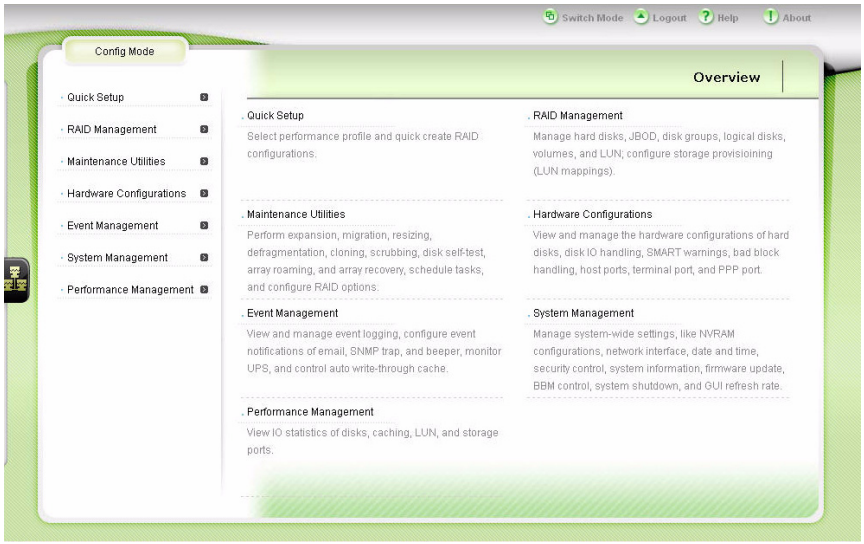

Switch Mode
Logout
Help
About
Config Mode
Overview
Quick Setup
RAID Management
Maintenance Utilities
Hardware Configurations
Event Management
System Management
Performance Management
Quick Setup
Select performance profile and quick create RAID configurations.
RAID Management
Manage hard disks, JBOD, disk groups, logical disks, volumes, and LUN; configure storage provisioining (LUN mappings).
Maintenance Utilities
Perform expansion, migration, resizing, defragmentation, cloning, scrubbing, disk self-test, array roaming, and array recovery, schedule tasks, and configure RAID options.
Hardware Configurations
View and manage the hardware configurations of hard disks, disk IO handling, SMART warnings, bad block handling, host ports, terminal port, and PPP port.
Event Management
View and manage event logging, configure event notifications of email, SNMP trap, and beeper, monitor UPS, and control auto write-through cache.
System Management
Manage system-wide settings, like NVRAM configurations, network interface, date and time, security control, system information, firmware update, BBM control, system shutdown, and GUI refresh rate.
Performance Management
View IO statistics of disks, caching, LUN, and storage ports.

Figure 2-18 Overview screen

The RAID GUI Config Mode provides the following configuration settings.

Quick Setup	Allows you to configure your array quickly.
RAID Management	Allows you to plan your array.
Maintenance Utilities	Allows you to perform maintenance tasks on your arrays.
Hardware Configurations	Allows you to configure the settings to hard disks, FC/SAS ports, and COM port settings.
Event Management	Allows you to configure event mail, event logs, and UPS settings.
System Management	Allows you to erase or restore the NVRAM configurations, set up the mail server, update the firmware and boot code and so on.
Performance Management	Allows you to check the IO statistics of hard disks, caches, LUNs, and FC/SAS ports.

Before configuration, read “Understanding RAID” thoroughly for RAID management operations.

2.5 Quick Setup

2.5.1 Performance profile

The RAID GUI provides three performance profiles for you to apply the preset settings to the RAID configuration. This allows users to achieve the optimal performance for a specified application. When using a profile for the RAID configuration, any attempt to change the settings is rejected. See the following table for the values of each profile. Select **Off** if you want to configure the settings manually.

Profile	AV streaming	Maximum IO per second	Maximum throughput
Disk IO Retry Count	0 (Degrade: 2)	1	1
Disk IO Timeout (second)	3 (Degrade: 10)	30	30
Bad Block Retry	Off	On	On
Bad Block Alert	On	N/A	N/A
Disk Cache	On	On	On
Write Cache	On	On	On
Write Cache Periodic Flush (second)	5	5	5
Write Cache Flush Ratio (%)	45	45	45
Read Ahead Policy	Adaptive	Off	Adaptive
Read Ahead Multiplier	8	-	16
Read Logs	32	-	32

Table 2-9 Performance profile values

NOTE

When the disks are in the degraded mode with the AV streaming profile selected, the disk IO retry count and timeout values may be changed to reduce unnecessary waiting for I/O completion.

2.5.2 RAID setup

To perform quick setup, all hard disks must be on-line and unused. Users can specify the RAID level, number of spare disks, and initiation method for an easy RAID configuration. See the following for details of each option.

HDD Information	This shows the number and the minimum size of hard disks.
RAID Level	RAID 0 / RAID 3 / RAID 5 / RAID 6 / RAID 10 / RAID 30 / RAID 50 / RAID 60
Spare Disks	Select the required number of global spare disks.
Initialization Option	**Background:** The controller starts a background task to initialize the logical disk by synchronizing the data stored on the member disks of the logical disk. This option is only available for logical disks with parity-based and mirroring-based RAID levels. The logical disk can be accessed immediately after it is created. **Noinit:** No initialization process, and the logical disk can be accessed immediately after it is created. There is no fault-tolerance capability even for parity-based RAID levels.

- **Single-controller RAID configuration**

A volume (for raid30, raid50, or raid60) or a logical disk (for other RAID levels) will be created with all capacity of all disks in the RAID enclosure. It will be mapped to LUN 0 of all host ports. All other configurations will remain unchanged, and all RAID parameters will use the default values.

- **Redundant-controller RAID configuration**

Two volumes (for raid30, raid50, or raid60) or two logical disks (for other RAID levels) will be created with all capacity of all disks in the RAID enclosure. One volume will be based on two disk groups, so totally there will be four disk groups. The preferred controller of one volume or logical disk is assgined to controller A and the other is assigned to controller B. They will be mapped to LUN 0 and LUN 1 of all host ports on both controllers. All other configurations will remain unchanged, and all RAID parameters will use the default values.

2.6 RAID Management

2.6.1 Hard disks

This feature allows you to add or remove hard disks and set any online disk as global spare drive. The hard disk information included is listed as follows.

Table 2-10 Hard disk information

Category	Display
HDD ID	Hard disk identifier
Model	Hard disk model name
Capacity (GB)	Hard disk capacity
State	On-line, Foreign, Conflict, Removed, PRemoved, Faulty, Initializing, Unknown.
Type	Unused, JBOD disk, DG data disk, Local spare, Global spare, or Clone target
SMART Status	Healthy, Alert, or Not supported
Mode	Ready, Standby, or Unknown

- **State definition**

On-line: The hard disk remains online when it is working properly.

Foreign: The hard disk is moved from another controller.

Conflict: The hard disk may have configurations that conflict with controller configurations.

Removed: The hard disk is removed.

PRemoved: The hard disk is permanently removed.

Faulty: The hard disk becomes faulty when a failure occurs.

Initializing: The hard disk starts the initialization.

Unknown: The hard disk is not recognized by the controller.

- **Mode definition**

Ready: The hard disk is in use or ready for use.

Standby: The hard disk is in standby mode.

Unknown: The hard disk is not recognized by the controller.

- **Buttons**

Add: To add hard disks, select a hard disk and click this button.

Remove: To remove hard disks, select a hard disk and click this button. To remove hard disks permanently, check the **Permanent remove** box when removing them.

Modify: Select a hard disk and click this button to enter the settings screen to enable or disable the disk cache and the disk identify function.

NOTE

1. When the selected hard disk is not in the on-line state, the Disk Cache field will not be displayed.
2. If a hard disk belongs to a disk group, you cannot change its disk cache. To modify it, refer to **2.6.3 Disk groups**.
3. If the hard disk belongs to a disk group, you can check the **'Apply to all members of this DG'** option to apply the disk identify setting to all the member disks in a disk group.
4. The **Disk Identify** can let controller correctly identify a hard disk even when they are moved from one slot to another at system power off time, and the configurations for the disks can be restored.

G.Spare: To add or remove global spare disks, click this button to enter the settings screen.

- **Detailed hard disk information**

Click to display a complete list of hard disk information. You will see the following details.

- HDD ID
- UUID
- Physical Capacity (KB)
- Physical Type
- Transfer Speed
- Disk Cache Setting
- Disk Cache Status
- Firmware Version
- Serial Number
- WWN
- NCQ Supported
- NCQ Status
- Command Queue Depth
- Standard Version Number
- Reserved Size of Remap Bad Sectors
- Bad Sectors Detected
- Bad Sectors Reallocated
- Disk Identify

2.6.2 JBOD

This feature allows you to create, delete, and modify your JBOD settings.

- **Create JBOD disks**

Click **Create** to add a new JBOD disk, where up to a maximum of 16 JBOD disks can be created. Specify the following options for the configuration.

JBOD ID	Select a JBOD ID from the drop-down menu.
Name	Use the system default name as **jbd**x. 'x' is the JBOD identifier. OR Uncheck the '**Use system default name**' box and enter the name in the **Name** field. The maximum name length is 63 bytes.
Member Disk	Select a corresponding hard disk to be used for JBOD from the drop-down menu.
Preferred Controller	*This option is only available when the redundant-controller system is in use.* Select the preferred controller to be in charge of managing and accessing the JBOD disk.

- **Delete JBOD disks**

Select the JBOD disk(s) you want to delete and click **Delete**. To delete all LUNs of **jbd**x, check the '**Force to delete LUN mapping(s)**' box. All access to the JBOD will be stopped.

- **Modify JBOD disks**

To modify a setting, select a JBOD and click **Modify**. Specify the following options for configuration.

Name	Type a name for the JBOD ID.
Preferred Controller	*This option is only available when the redundant-controller system is in use.* Select the preferred controller to be in charge of managing and accessing the JBOD disk. However, the controller ownership will not change unless you check the **'Change owner controller immediately'** box.
Write Cache	This option enables or disables the write cache of a JBOD disk.

Write Sorting	This option enables or disables the sorting in the write cache. To improve writing performance, it is recommended to turn this option on for random access. This option is available only if the write cache is on.
Read Ahead Policy	**Always:** The controller performs pre-fetching data for every read command from hosts. **Adaptive:** The controller performs pre-fetching only for host read commands that are detected as sequential reads. The detection is done by read logs. **Off:** If there is no sequential read command, read-ahead will result in overhead, and you can disable the read-ahead.
Read Ahead Multiplier	This option specifies the read ahead multiplier for the **Always** and **Adaptive** read ahead policies. Select how much additional sequential data will be pre-fetched. The default value is 8.
Read Logs	This option specifies the number of read logs for the **Adaptive** read ahead policy. The range is between 1 and 128. The default value is 32.

To clear write buffers in the write cache of a JBOD disk, select a JBOD and click the **Flush** button.

- ## Create JBOD volume pair

Instead of creating volume pairs in the **Snapshot Volumes** page, you can directly create volume pair to a specified JBOD disk by clicking the **S.VOL** button. Specify a virtual disk as the secondary volume from the **SV ID** drop-down menu, then click the **Apply** button to confirm.

- ## Detailed JBOD disk information

Click to display a complete list of JBOD disk information. You will see the following details.

- JBOD ID
- UUID
- Created Time and Date
- Write Cache Status
- Write Cache Setting
- Write Sorting
- Read Ahead Policy
- Read Ahead Multiplier
- Read Logs

2.6.3 Disk groups

This feature allows you to create, delete, and modify your disk group settings.

- Create disk groups

Click **Create** to add a new disk group, where up to a maximum of 8 disk groups can be created. Specify the following options for configuration.

DG ID	Select a DG ID from the drop-down menu.
Name	Use the system default name as **dg**x. 'x' is the DG identifier. OR Uncheck the '**Use system default name**' box and enter the name in the **Name** field. The maximum name length is 63 bytes.
Members and Spares	Select member disks and spare disks to be grouped.
Capacity to Truncate (GB)	Specifies the capacity to be truncated for the smallest disk of this disk group. This option is useful when the replacement disk that is slightly smaller than the original disk. Without this option, the capacity to truncate is 0GB.
LD Initialization Mode	The initialization mode defines how logical disks of a disk group are initialized. Different disk groups can have different initialization modes. **Parallel:** The initialization tasks of logical disks are performed concurrently. **Sequential:** Only one initialization task is active at a time.
Write-zero immediately	When enabled, this function will start a background task to write zero to all member disks of the created disk group. The disk group can be used for logical disks only after this process is completed.

NOTE

The minimum number of member disks in a disk group is two. Different disk groups may have a different number of member disks. The number of member disks also determines the RAID level that can be used in the disk group.

- **Delete disk groups**

  Select the disk group(s) you want to delete and click **Delete**.

- **Modify disk groups**

  To modify a setting, select a DG and click **Modify**. Specify the following options for configuration.

Name	Type a name associated for the DG ID.
Spare Disks	Assign disks to be used as local spares.
Disk Cache	This option enables or disables the on-disk cache of hard disks in a disk group. When a new disk becomes a member of the disk group (for example, by disk rebuilding and cloning); the on-disk cache uses the same settings as the disk group.
LD Initialization Mode	The initialization mode defines how logical disks of a disk group are initialized. Different disk groups can have different initialization modes. **Parallel:** The initialization tasks of logical disks are performed concurrently. **Sequential:** Only one initialization task is active at a time.
LD Rebuild Mode	This determines how to rebuild logical disks in a disk group. All logical disks can be rebuilt at the same time or one at a time. Different disk groups can have different rebuild modes. **Parallel:** The rebuilding tasks are started simultaneously for all logical disks in the disk group. The progress of each rebuilding task is independent from each other. **Sequential:** Rebuilding always starts from the logical disk with the smallest relative LBA on the disk group, continues to the logical disk with the second smallest relative LBA, and so on. **Prioritized:** Similar to sequential rebuild mode, this rebuilds one logical disk at a time, but the order of logical disks to be rebuilt can determined by users.
Rebuild Task Priority	**Low / Medium / High** This option sets the priority of the background task for disk rebuild of disk groups.

Initialization Task Priority	**Low / Medium / High** This option sets the priority of the background tasks for logical disk initialization of disk groups.
Utilities Task Priority	**Low / Medium / High** This option sets the priority of the background tasks for utilities of disk groups. These include RAID reconfiguration utilities and data integrity maintenance utilities.

NOTE

1. Progress rates increase in proportion to priority (i.e. A high priority task runs faster than a low priority one.)
2. When there is no host access, all tasks (regardless of priority) run at their fastest possible speed.
3. When host access exists, tasks run at their minimum possible speed.

- **Detailed disk group information**

Click to display a complete list of disk group information. You will see the following details.

- DG ID
- UUID
- Created Time and Date
- Disk Cache Setting
- LD Initialization Mode
- LD Rebuild Mode
- LD Rebuild Order
- Rebuild Task Priority
- Initialization Task Priority
- Utilities Task Priority
- Member Disk's Layout
- Original Member Disks

2.6.4 Logical disks

This feature allows you to create, delete, and modify your logical disk settings.

- **Create logical disks**

Click **Create** to add a new logical disk, where up to a maximum of 32 logical disks can be created in each DG. Specify the following options for configuration.

DG ID	Select a DG ID from the drop-down menu. This is the disk group to be assigned for logical disk setting.
LD ID	Select an LD ID from the drop-down menu.

Name	Use the system default name as **dg**x**ld**y. 'x' is the DG identifier and 'y' is the LD identifier. OR Uncheck the '**Use system default name**' box and enter the name in the Name field. The maximum name length is 63 bytes.
RAID Level	Select a RAID level for the logical disk. Different logical disks in a disk group can have different RAID levels. However, when NRAID is selected, there must be no non-NRAID logical disks in the same disk group.
Capacity (MB)	Enter an appropriate capacity for the logical disk. This determines the number of sectors a logical disk can provide for data storage.
Preferred Controller	*This option is only available when the redundant-controller system is in use.* Select the preferred controller to be in charge of managing and accessing the logical disk.
Stripe Size (KB)	**4 / 8 / 16 / 32 / 64 / 128 / 256 / 512** The stripe size is only available for a logical disk with a striping-based RAID level. It determines the maximum length of continuous data to be placed on a member disk. The stripe size must be larger than or equal to the cache unit size.
Free Chunk	Each free chunk has a unique identifier in a disk group, which is determined automatically by the controller when a free chunk is created. Select a free chunk from the drop-down menu for logical disk creation.
Initialization Option	**Noinit:** No initialization process, and the logical disk can be accessed immediately after it is created. **Regular:** The controller initializes the logical disk by writing zeros to all sectors on all member disks of the logical disk. This ensures that all data in the logical disks are scanned and erased. **Background:** The controller starts a background task to initialize the logical disk by synchronizing the data stored on the member disks of the logical disk. This option is only available for logical disks with parity-based and mirroring-based RAID levels.

Alignment Offset (sector)	Set the alignment offset for the logical disk starting sector to enhance the controller's performance. For Windows OS, it is suggested to set the alignment offset at sector 63.

NOTE

Make sure the disk group to be created for a new logical disk is in OPTIMAL or LD_INIT state, otherwise the new logical disk will not be created.

- **Delete logical disks**

Select the logical disk(s) you want to delete and click **Delete**. To delete all LUNs of **dg**x**ld**y, check the '**Force to delete LUN mapping(s)**' box. All access to the logical disk will be stopped.

- **Modify logical disks**

To modify a setting, select an LD and click **Modify**. Specify the following options for configuration.

Name	Type a name for the DG ID/ LD ID.
Preferred Controller	*This option is only available when the redundant-controller system is in use.* Select the preferred controller to be in charge of managing and accessing the logical disk. However, the controller ownership will not change unless you check the **'Change owner controller immediately'** box.
Write Cache	This option enables or disables the write cache of a logical disk.
Write Sorting	This option enables or disables the sorting in the write cache. To improve writing performance, it is recommended to turn this option on for random access. This option is available only if the write cache is on.
Read Ahead Policy	**Always:** The controller performs pre-fetching data for every read command from hosts. **Adaptive:** The controller performs pre-fetching only for host read commands that are detected as sequential reads. The detection is done by read logs. **Off:** If there is no sequential read command, read-ahead will result in overhead, and you can disable the read-ahead.

Read Ahead Multiplier	This option specifies the read ahead multiplier for the **Always** and **Adaptive** read ahead policies. Select how much additional sequential data will be pre-fetched. The default value is 8.
Read Logs	This option specifies the number of concurrent sequential-read streams for the **Adaptive** read ahead policy, and the range is between 1 and 128. The default value is 32.
LD Read Algorithm	This option is only available for logical disks with parity-based RAID level, i.e. RAID 3/5/6. **None:** None of the algorithms will be used when accessing data disks. **Intelligent Data Computation:** The controller will access logical disks within the shortest response time. This greatly enhances read performance. **Fast Read Response:** When this option is selected, you are prompted to enter the maximum response time for all read requests. The allowed range for response time is 100 to 15000 msecs. **Check on Read:** This option is similar to the Fast Read Response. In addition to reading the requested data from disks, the controller will also perform parity check across corresponding strips on each data disk.

To clear write buffers in the write cache of a logical disk, select a logical disk and click the **Flush** button.

- Create logical disk (LD) snapshot volume pair

Instead of creating volume pairs in the **Snapshot Volumes** page, you can directly create volume pair to a specified logical disk by clicking the **S.VOL** button. Specify a virtual disk as the secondary volume from the **SV ID** drop-down menu, then click the **Apply** button to confirm.

- **Detailed logical disk information**

Click to display a complete list of logical disk information. You will see the following details.

- DG ID
- LD ID
- UUID
- Created Time and Date
- LD Read Algorithm
- Alignment Offset (sector)
- Write Cache Status
- Write Cache Setting
- Write Sorting
- Read Ahead Policy
- Read Ahead Multiplier
- Read Logs
- Member State

2.6.5 Volumes

This feature allows you to create, delete, and modify your volume settings. RAID 30/50/60 are supported by creating striping volumes over RAID 3/5/6 logical disks.

- **Create volumes**

Click **Create** to add a new volume, where up to a maximum of 32 volumes can be created. Specify the following options for the configuration.

VOL ID	Select a VOL ID from the drop-down menu.
Name	Use the system default name as **vol**x. 'x' is the VOL identifier. OR Uncheck the '**Use system default name**' box and enter the name in the **Name** field. The maximum name length is 63 bytes.
LD Level	Select a RAID level to filter a list of member LDs.
LD Owner Controller	*This option is only available when the redundant-controller system is in use.* Select the owner controller of the member LDs. Only the LDs whose owner controller are equal to the specified will be filtered out in "Member LDs".
Member LDs	Select the LDs to be grouped.
Preferred Controller	*This option is only available when the redundant-controller system is in use.* Select the preferred controller to be in charge of managing and accessing the volume.

Stripe Size (KB)	**4 / 8 / 16 / 32 / 64 / 128 / 256 / 512** The stripe size must be larger than or equal to the cache unit size.
Alignment Offset (sector)	Set the alignment offset for volume starting sector to enhance the controller's performance. For Windows OS, it is suggested to set the alignment offset at sector 63.

NOTE

1. All logical disks must be in the same RAID level.
2. No two logical disks can be in the same disk group.
3. None of the logical disks can be used by other volumes.
4. None of the logical disks can be bound to any LUNs.
5. All logical disks must be in the optimal state.
6. All disk groups of the logical disks must belong to the same owner controller.

- **Delete volumes**

Select the volume(s) you want to delete and click **Delete**. To delete all LUNs of **vol**x, check the '**Force to delete LUN mapping(s)**' box. All access to the volume will be stopped.

- **Modify volumes**

To modify a setting, select a volume and click **Modify**. Specify the following options for configuration.

Name	Type a name for the volume ID.
Preferred Controller	*This option is only available when the redundant-controller system is in use.* Select the preferred controller to be in charge of managing and accessing the volume. However, the controller ownership will not change unless you check the **'Change owner controller immediately'** box.
Write Cache	This option enables or disables the write cache of a volume.
Write Sorting	This option enables or disables the sorting in the write cache. To improve writing performance, it is recommended to turn this option on for random access. This option is available only if the write cache is on.

Read Ahead Policy	**Always:** The controller performs pre-fetching data for every read command from hosts. **Adaptive:** The controller performs pre-fetching only for host read commands that are detected as sequential reads. The detection is done by read logs. **Off:** If there is no sequential read command, read-ahead will result in overhead, and you can disable the read-ahead.
Read Ahead Multiplier	This option specifies the read ahead multiplier for the **Always** and **Adaptive** read ahead policies. Select how much additional sequential data will be pre-fetched. The default value is 8.
Read Logs	This option specifies the number of concurrent sequential-read streams for the **Adaptive** read ahead policy, and the range is between 1 and 128. The default value is 32.

To clear write buffers in the write cache of a volume, select a volume and click the **Flush** button.

- ## Create volume (VOL) snapshot volume pair

Instead of creating volume pairs in the **Snapshot Volumes** page, you can directly create volume pair to a specified volume by clicking the **S.VOL** button. Specify a virtual disk as the secondary volume from the **SV ID** drop-down menu, then click the **Apply** button to confirm.

- ## Detailed volume information

Click to display a complete list of volume information. You will see the following details.

- VOL ID
- UUID
- Created Time and Date
- Alignment Offset (sector)
- Write Cache Status
- Write Cache Setting
- Write Sorting
- Read Ahead Policy
- Read Ahead Multiplier
- Read Logs

2.6.6 Snapshot Volumes

This feature allows you to create, delete, and modify your snapshot volume settings. This is referred as the snapshot technology. See **5.4 Snapshot on page 5-38** for more information.

- ### Create snapshot volume pairs (S.VOL.Pair)

Click **Add** to add a new snapshot volume pair before adding new snapshot volumes, where up to a maximum of 64 volume pairs can be created. Specify the following options for the configuration.

PVID	From the drop-down menu, specify an LD as the primary volume of the volume pair.
SVID	From the drop-down menu, specify an LD as the secondary volume of the volume pair.

- ### Delete snapshot volume pairs

Select the snapshot volume pair(s) you want to delete and click **Remove**.

- ### Modify snapshot volume pairs

To modify a setting, select a snapshot volume and click **Modify**. Specify the following options for configuration.

Overflow Alert (%)	Specify an overflow alert threshold for a secondary volume. The range is from 50 to 99. When the allocated space exceeds the specified threshold, an alert notification is generated. If not specified, the default threshold is 80. To configure the same settings to all snapshot volume pairs, check the '**Apply to all volume pairs**' box.

- ### Expanding the capacity of snapshot volume pairs

To expand the capacity of a snapshot volume pairs, do the following:

1. Click **Expand** and specify the following options for an secondary volume expansion task.

Capacity (MB)	The capacity of a logical disk can be expanded if there is a free chunk available on the disk group.
Schedule	**Immediately:** The task will start immediately. **Once:** The task will start on the specified date and time.

Starting Free Chunk / Ending Free Chunk	This option specifies the start and end of free chunks to be used for the expansion. The **Ending Free Chunk** must be bigger than or equal to the **Starting Free Chunk**.

NOTE

At least one free chunk must be adjacent to the logical disk.

Initialization Option	**Background / Noinit** Background applies only to the logical disks with parity-based RAID level or mirroring-based RAID level.

- **Detailed snapshot volume pair information**

  Click to display a complete list of snapshot volume pair information. You will see the following details.

  - PV ID
  - SV ID
  - Overflow Alert(%)

- **Create Spare COW volumes (S.COW.VOL)**

  Click **Add** to add a new spare COW volume, where up to a maximum of 128 volume pairs can be created. Specify the following options for the configuration.

COW VOL ID	From the drop-down menu, specify an LD as the spare COW volume.

- **Delete snapshot volume pairs**

  Select the spare COW volume you want to delete and click **Remove**.

- **Create snapshot volumes**

  Click **Create** to add a new snapshot volume, where up to 4 snapshot volumes can be created per primary volume (snapshot volumes). The total maximum number of snapshot volumes that can be created is 64. Specify the following options for the configuration.

SVOL ID	Select a snapshot volume ID from the drop-down menu.
PV ID	Select a primary volume ID from the drop-down menu.

Name	Use the system default name as **svol**x. 'x' is the VOL identifier. OR Uncheck the '**Use system default name**' box and enter the name in the **Name** field. The maximum name length is 63 bytes.

- **Delete snapshot volumes**

Select the snapshot volume(s) you want to delete and click **Delete**. To delete all LUNs of **svol**x, check the '**Force to delete LUN mapping(s)**' box. All access to the snapshot volume will be stopped.

- **Modify snapshot volumes**

To modify a setting, select a snapshot volume and click **Modify**. You can type a name for the specified snapshot volume.

- **Restore to snapshot volumes**

To restore the primary volume to a snapshot volume in a volume pair. Select a snapshot volume and click **Restore**.

- **Detailed snapshot volume information**

Click to display a complete list of snapshot volume information. You will see the following details.

- VOL ID
- UUID
- Allocated Space on SV (MB)

2.6.7 Storage provisioning

The RAID GUI provides three storage provision methods; simple, symmetric, and selective. Whenever you change the method, the following confirmation message is displayed.

Switch Storage Provision Method
Changing the storage presentation method is allowed only when all LUN mappings are cleared. Do you want to continue?
Confirm
Cancel

Figure 2-19 Method switching message

- **Simple method**

Simple storage is used in direct attached storage (DAS) environments, where there is no FC switch between the RAID and the hosts.

As the illustration shows, any computer is allowed to access the LUNs presented by the controller after gaining access to the host ports of the controller.

LUNs are assigned to each virtual disk in RAID so the host can address and access the data in those devices.

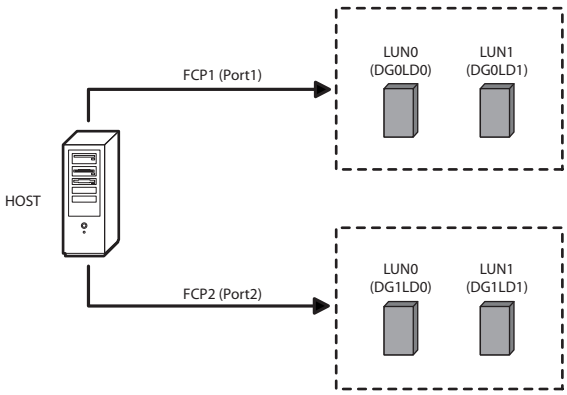


Figure 2-20 Simple storage

Add LUNs in a storage port

In the simple storage main screen, click **Add** to add a LUN to the default storage group of an FC port/SAS port/SCSI port, **fcp**x/**sas**y/**scp**z, with a virtual disk.

HTP ID	Each FC/SAS/SCSI port has a unique ID, which is determined according to the physical location of the port on the controller. Select one from the drop-down menu.
SCSI ID	(For SCSI port) Select a SCSI ID from the drop-down menu. A maximum of 16 SCSI IDs can be added to the controller.
LUN ID	Select a LUN ID from the drop-down menu, where up to a maximum of 128 LUNs can be selected.
Mapping Virtual Disk	Select a virtual disk from the drop-down menu for LUN mapping.
Sector Size	**512Byte / 1KB / 2KB / 4KB** Select a sector size from the drop-down menu as the basic unit of data transfer in a host.
Number of Cylinder / Number of Head / Number of Sector	Define a specific cylinder, head, and sector to accommodate different host systems and applications. The default is **Auto**.

Write Completion	**Write-behind:** Write commands are reported as completed when a host's data is transferred to the write cache. **Write-through:** Write commands are reported as completed only when a host's data has been written to disk.

Remove LUNs in storage port

Select the LUN(s) you want to remove and click **Remove**. To remove all LUNs of a virtual disk from the default storage group of **fcp**x/**sas**y/**scp**z, check the '**Remove mapping virtual disk from all storage group**' box.

- **Symmetric method**

Symmetric storage is used in environments where hosts are equipped with multi-path IO (MPIO) driver or software that can handle multiple paths (LUNs) to a single virtual disk. Use the provided PathGuard package to install and use the MPIO driver. For more information, see **5.1 Multi-Path IO Solutions**.

In this case, the controller's performance is highly elevated. You need not consider different host ports because the bindings between hosts and storage groups are applied to all host ports.

As the illustration shows, LUNs are assigned according to each host's WWPN (World Wide Port Name). Therefore, you need to set the host WWPN first. Each host can recognize LUNs as paths to virtual disks, instead of individual disks.

To set up symmetric storage groups, first add host(s).

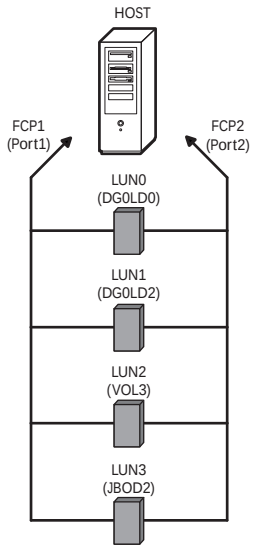


Figure 2-21 Symmetric storage

Add hosts

In the symmetric storage main screen, click **Host** > **Add**.

Host ID	Select a Host ID from the drop-down menu. A maximum of 32 hosts can be added to the controller.

WWPN	Each FC port needs a WWPN for communicating with other devices in an FC domain. Users can choose each WWPN of Fiber HBA from the '**Choose from detected hosts**' box or directly enter the WWPN in this field.
SAS Address	For SAS controller each SAS port needs a SAS Address for communicating with other devices in an SAS domain.
Host Name	Use the system default name as **host**x. 'x' is the Host identifier. OR Uncheck the '**Use system default name**' box and enter the name in the **Name** field. The maximum name length is 63 bytes.
HG ID	Select a Host Group ID from the drop-down menu. You can select from hg0 to hg31 or No group.That is must to set for symmetric method.

Remove hosts

Select the host(s) you want to delete and click **Remove**. Check the '**Only remove from host group**' box if you want to remove the host(s) from the host group only.

Modify hosts/host group

Select a host you want to change for its host name, host group ID, or host group name, and click **Modify** to enter the settings screen.

Add LUNs in Host Group

After setting the host(s), click **Back** to return to the symmetric storage main screen. Then click **Add** to add LUNs in the HG(s).

HG ID	Select a HG ID from the drop-down menu. A maximum of 32 hosts can be added to the controller.
LUN ID	Select a LUN ID from the drop-down menu. where up to 128 IDs are available for the selection.
Mapping Virtual Disk	Select a virtual disk from the drop-down menu for LUN mapping.

Sector Size	**512Byte / 1KB / 2KB / 4KB** Select a sector size from the drop-down menu as the basic unit of data transfer in a host.
Number of Cylinder / Number of Head / Number of Sector	Define a specific cylinder, head, and sector to accommodate different host systems and applications. The default is **Auto**.
Write Completion	**Write-behind:** Write commands are reported as completed when host's data is transferred to the write cache. **Write-through:** Write commands are reported as completed only when host's data has been written to disk.

Remove LUNs from host

Select the LUN(s) you want to remove and click **Remove**. To remove all LUNs of a virtual disk from one or all hosts, check the '**Remove mapping virtual disk from all host**' box.

- **Selective method**

Selective storage is used in complicated SAN environments, where there are multiple hosts accessing the controller through an FC switch. This method provides the most flexibility for you to manage the logical connectivity between host and storage resources exported by the controller.

As the illustration shows, the HG (Host Group) can be a host or a group of hosts that share the same access control settings in the controller. SG represents the LUNs as a storage group. Bind the host/ host group and storage group to the same host port.

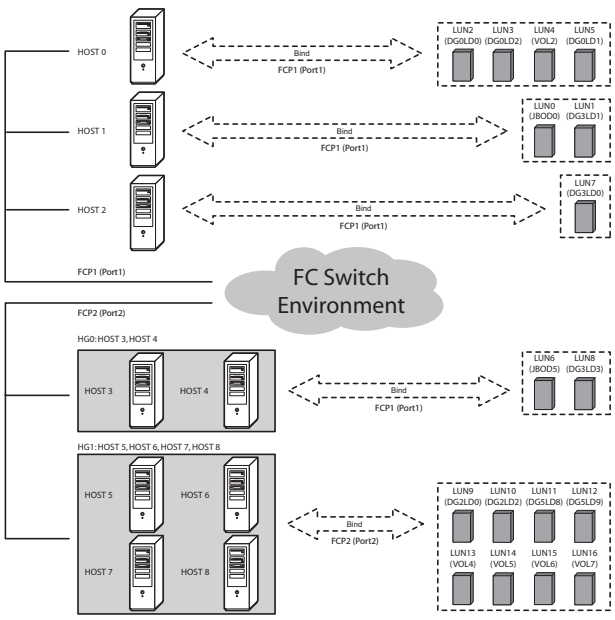


Figure 2-22 Selective storage

Add hosts

In the selective storage main screen, click **Host** > **Add**.

Host ID	Select a Host ID from the drop-down menu. A maximum of 32 hosts can be added to the controller.
WWPN	Each FC port needs a WWPN for communicating with other devices in an FC domain. Users can choose each WWPN of Fiber HBA from the '**Choose from detected hosts**' box or directly enter the WWPN in this field.
SAS Address	For SAS controller each SAS port needs a SAS Address for communicating with other devices in an SAS domain.
Host Name	Use the system default name as **host**x. 'x' is the Host identifier. OR Uncheck the '**Use system default name**' box and enter the name in the **Name** field. The maximum name length is 63 bytes.
HG ID	Select a Host Group ID from the drop-down menu. You can select from hg0 to hg31 or No group.

Remove hosts

Select the host(s) you want to delete and click **Remove**. Check the '**Only remove from host group**' box if you want to remove the host(s) from the host group only.

Modify hosts/host groups

Select a host you want to change for its host name, host group ID, or host group name, and click **Modify** to enter the settings screen.

Add LUNs in storage group

In the selective storage main screen, click **SG** > **Add**.

SG ID	Select a SG ID from the drop-down menu. A maximum of 34 storage groups can be created in the controller.
LUN ID	Select a LUN ID from the drop-down menu, where up to 128 IDs are available for the selection. A total of 1024 LUNs can be created in the controller.

Mapping Virtual Disk	Select a virtual disk from the drop-down menu for LUN mapping.
Mask Status	**Unmask / Mask** This option makes a LUN available to some hosts and unavailable to other hosts.
Access Right	**Read-only / Read-writable** The access right is applied to individual LUNs in a storage group.
Sector Size	**512Byte / 1KB / 2KB / 4KB** Select a sector size from the drop-down menu as the basic unit of data transfer in a host.
Number of Cylinder / Number of Head / Number of Sector	Define a specific cylinder, head, and sector to accommodate different host systems and applications. The default is **Auto**.
Write Completion	**Write-behind:** Write commands are reported as completed when a host's data is transferred to the write cache. **Write-through:** Write commands are reported as completed only when a host's data has been written to disk.

Remove LUNs in storage group

Select the LUN(s) you want to delete and click **Remove**. To remove all LUNs of a virtual disk from all storage groups, check the '**Remove mapping virtual disk from all storage group**' box.

Modify LUN/storage group

Select a LUN/ storage group you want to change for its mask status, access right, or storage group name, and click **Modify** to enter the settings screen. To configure the same settings to all LUNs in a storage group, check the '**Apply to all LUNs in this storage group**' box.

Bind host/host group and storage group to host ports

Now you can click **Bind** in the selective storage main screen. Select from the **HTP ID**, **Host/ HGID**, and **SG ID** drop-down menu for binding.

Unbind hosts/ host groups and storage groups to host ports

Select a binding you want to cancel and click **Unbind** in the selective storage main screen. Click **Confirm** to cancel the selected binding.

2.7 Maintenance Utilities

This feature allows you to perform maintenance tasks on your arrays.

2.7.1 Expanding disk groups

DG Reconfiguration allows expansion on disk groups by adding one or more disks, thus increasing the usable capacity of the disk group. You can also perform defragmentation during expansion.

To expand disk groups, do the following:

1. Select **Maintenance Utilities > DG Reconfiguration** from the main menu.
2. Click **Expand** and specify the following options for a DG expansion task.

DG ID	Select a disk group for expansion from the drop-down menu.
Expanding HDDs	Select and use the arrow buttons to move one or more unused hard disks from the *Available HDDs* list to the *Expanding HDDs* list.
Schedule	**Immediately:** The task will start immediately. **Once:** The task will start on the specified date and time.
Defragment during expanding	Check this option to allow for defragmentation during expansion.

3. Click **Apply** to review the current settings.
4. Click **Confirm**. The task is created.

NOTE

1. The disk group to be expanded must be in the optimal state.
2. You may only select to increase the number of hard disks but not to change the disk group setting.
3. Once confirmed, please wait until the expansion process is complete. Do not change or select any functions during the expansion process.

2.7.2 Defragmenting disk groups

Except defragmenting disk groups during expansion, there is another way to perform the task.

1. Select **Maintenance Utilities > DG Reconfiguration** from the main menu.

2. Click **Defragment** and specify the following options for defragmenting.

DG ID	Select a disk group to defragment from the drop-down menu.
Schedule	**Immediately:** The task will start immediately. **Once:** The task will start on the specified date and time.

3. Click **Apply** to view the current settings.

4. Click **Confirm**. The task is created.

After defragmentation is complete, all free chunks will be consolidated into the one free chunk located in the space at the bottom of member disks.

NOTE

1. Defragmentation does not support NRAID disk group.
2. There must be free chunks and logical disks on disk groups.

2.7.3 Changing RAID level / stripe size for logical disks

LD Reconfiguration supports stripe size and RAID level migration for logical disks. You can conduct disk group expansion with migration at the same time.

To change the RAID level or stripe size of a logical disk, do the following:

1. Select **Maintenance Utilities > LD Reconfiguration** from the main menu.

2. Click **Migrate** and specify the following options for an LD migration task.

DG ID/LD ID	Select a DG ID and an LD ID from the drop-down menu for migration.
Expanding HDDs	The controller performs disk group expansion with specified hard disks.
RAID Level	The controller performs the specified RAID level migration. The feasibility of migration is limited to the original and final RAID level and the number of member disks in the disk group. The following table defines the rules of the number disks during the RAID migration.

Table 2-11 Limitations of the number of member disks

New \ Old	RAID 0	RAID 1	RAID 10	RAID 3/5	RAID 6
RAID 0	Nn ≥ No	OK	OK	OK	OK
RAID 1	N/A	Nn > No	N/A	N/A	N/A

Table 2-11 Limitations of the number of member disks

RAID 10	Nn ≥ No*2	OK	Nn ≥ No	Nn ≥ (No-1)*2	Nn ≥ (No-2)*2
RAID 3/5	Nn ≥ No+1	OK	OK	Nn ≥ No	OK
RAID 6	Nn ≥ No+2	OK	OK	Nn ≥ No+1	Nn ≥ No

* Where "Nn" means the number of member disks in the new RAID level, "No" means the number of member disks in the original/old RAID level, "OK" means the migration is always possible, and "N/A" means the migration is disallowed.

Stripe Size (KB)	This option must be specified when migrating from a non-striping-based RAID level to a striping-based RAID level.
Schedule	**Immediately:** The task will start immediately. **Once:** The task will start on the specified date and time.
Defragment during migration	Check this option to allow defragmentation during migration.

2.7.4 Expanding the capacity of logical disks in a disk group

To expand the capacity of a logical disk, do the following:

1. Select **Maintenance Utilities > LD Reconfiguration** from the main menu.
2. Click **Expand** and specify the following options for an LD expansion task.

DG ID/LD ID	Select a DG ID and an LD ID from the drop-down menu for expansion.
Capacity (MB)	The capacity of a logical disk can be expanded if there is a free chunk available on the disk group.

NOTE

1. The new capacity must be bigger than the current capacity.
2. The sum of increased capacity of all logical disks on the disk group must be less than or equal to the sum of capacity of all selected free chunks.

Schedule	**Immediately:** The task will start immediately. **Once:** The task will start on the specified date and time.
Starting Free Chunk / Ending Free Chunk	This option specifies the start and end of free chunks to be used for the expansion. The **Ending Free Chunk** must be bigger than or equal to the **Starting Free Chunk**.

NOTE
At least one free chunk must be adjacent to the logical disk.

Initialization Option	**Background / Noinit** Background applies only to the logical disks with parity-based RAID level or mirroring-based RAID level.

3. Click **Apply** to view the current settings.
4. Click **Confirm**. The task is created.

2.7.5 Shrinking logical disks

The shrink operation conducts without background task; it simply reduces the capacity of the logical disk.

To release free space of a logical disk on a disk group, do the following:

1. Select **Maintenance Utilities > LD Reconfiguration** from the main menu.
2. Click **Shrink** and specify the following options for an LD shrink task.

DG ID/LD ID	Select a DG ID and an LD ID from the drop-down menu for shrink.
Capacity (MB)	Enter the new capacity for the specified logical disk to be shrunk. Note that the new capacity must be higher than zero.

NOTE
It is advised that the file systems on the host be shrunk before shrinking the logical disks; otherwise shrinking might cause data loss or file system corruption.

3. Click **Apply** to view the current settings.
4. Click **Confirm**. The task starts.

2.7.6 Expanding volumes

To expand the capacity of a volume, do the following:

1. Select **Maintenance Utilities > VOL Reconfiguration** from the main menu.
2. Select **Expand** and specify the following options for a VOL expansion task. The expansion volume is formed by concatenating new logical disks.

VOL ID	Select a VOL ID from the drop-down menu for expansion.
LD Level	Select a RAID level to filter a list of expanding LDs.

Expanding LDs	Select and use the arrow buttons to move one or more LDs from the *Available LDs* list to the *Expanding LDs* list.

NOTE

1. The volume must be in optimal state.
2. The maximum number of member logical disks for each volume is eight.
3. No two logical disks can be in the same disk group.
4. None of the logical disks can be used by other volumes.
5. None of the logical disks can be bound to any LUNs.
6. All logical disks must be in the optimal state.
7. All disk groups of the logical disks must belong to the same owner controller.

3. Click **Apply** to view the current settings.
4. Click **Confirm** to continue the expansion.

2.7.7 Shrinking volumes

The shrink operation conducts without background task; it simply reduces the capacity of the volume by removing the concatenating volume units.

To release free space of a volume, do the following:

1. Select **Maintenance Utilities > LD Reconfiguration** from the main menu.
2. Select **Shrink** and specify the following options for a VOL shrink task.

VOL ID	Select a VOL ID from the drop-down menu for shrink.
Shrinking VUs	Select member VUs you want to remove from the list and use the arrow buttons to move them to the *Shrinking VUs* list.

NOTE

1. The volume must be in optimal state.
2. There must be at least two concatenating volume units in a volume.
3. All selected volume units must be the last concatenating volume units in the volume.

3. Click **Apply** to view the current settings.
4. Click **Confirm** to continue the shrink.

2.7.8 Cloning hard disks

When a hard disk is likely to become faulty or develop errors, for example, when the number of reported errors or bad sectors of a physical disk increases over a certain threshold, or a disk reports SMART warning, you can copy all the data on the disk to another disk.

To clone a hard disk, do the following:

1. Select **Maintenance Utilities > HDD Clone** from the main menu.
2. Click **Clone** and specify the following disk cloning options.

Source Disk	Select a source disk you want to clone. The disk must not be in an NRAID disk group.
Target Disk	Select the target disk to be the clone. The disk must be either unused, a global spare, or a local spare of the same disk group as the **Source Disk**.
Schedule	**Immediately:** The task will start immediately. **Once:** The task will start on the specified date and time.
Automatic Resume	During cloning, if the target disk fails, the controller will use another disk and resume cloning. [The **Auto Spare Control** option (see **2.7.16 Miscellaneous on page 2-55**) must be set to On.] The following is the order of disks used to resume cloning: 1. Local spare disks 2. Global spare disks 3. Unused disks If there is no disk to resume cloning, or this option is not specified, cloning is aborted when the target disk fails.

NOTE

1. If there is disk scrubbing task or parity regeneration task in the disk group of the source disk, the task is aborted and cloning is started.
2. If the disk group of the source disk contains faulty disks, cloning is suspended until the disk group completely rebuilds its disks.

3. Click **Apply**. The task will start according to the specified time.

To cancel hard disk cloning, do the following:

1. Select the task(s) and click **Stop** to abort disk cloning. A confirmation prompt displays. Click **Confirm** to cancel the cloning task.

The target disk will become an unused disk. If there is a degraded disk group and auto-spare option is on, the target disk will be used for rebuilding.

2.7.9 Scrubbing

This feature supports parity check and recovery for disk groups, logical disks, and hard disks. Bad sectors will be reported when detected.

To perform disk scrubbing on a disk group, do the following:

1. Select **Maintenance Utilities > Scrubbing** from the main menu.
2. Click **Scrub** and specify the following options for a disk scrubbing task.

Target Type	Select either **HDD** or **DG** as the scrubbing disk type. **HDD:** Specify an HDD ID for scrubbing. **DG:** Specify a DG ID and an LD ID/All LDs for scrubbing.
Parity Check	This option is only available for parity-based RAID level LDs. **None:** No parity check is performed. **Check Only:** The controller checks the parity for logical disks. **Regenerate:** Any parity inconsistency detected is regenerated by the controller.
Schedule	**Immediately:** The task will start immediately. **Once:** The task will start on the specified date and time. **Weekly:** The task will start on the specified day and time every week. **Monthly:** The task will start on the specified date and time every month.

3. Click **Apply**. The task will start according to the specified time.

NOTE

1. The hard disk must not be a member disk of a disk group.
2. The disk group and logical disk(s) for scrubbing must be in the optimal state.
3. The scrubbing task will be aborted if the disk group enters degraded mode, starts rebuilding disk, or starts disk cloning.
4. If the disk group of the source disk contains faulty disks, scrubbing is aborted until the disk group completely rebuilds its disks.

To cancel disk scrubbing, do the following:

1. Select the task(s) and click **Stop** to abort the disk scrubbing. A confirmation prompt displays. Click **Confirm** to cancel the scrubbing task.

2.7.10 Regenerating the parity

This feature is less complicated than scrubbing. This command regenerates the parity of a logical disk or all logical disks on disk groups without parity checking. Follow the steps below to create a regenerating parity task.

1. Select **Maintenance Utilities > Regenerate Parity** from the main menu.
2. Click **Reg-parity** and specify the following options for a parity regeneration task.

DG ID/LD ID	Select a DG ID and an LD ID or All LDs from the drop-down menu for parity regeneration.
Schedule	**Immediately:** The task will start immediately. **Once:** The task will start on the specified date and time. **Weekly:** The task will start on the specified day and time every week. **Monthly:** The task will start on the specified date and time every month.

3. Click **Apply**. The task will start according to the specified time.

To stop parity regeneration, do the following:

1. Select the task(s) and click **Stop**. A confirmation prompt displays. Click **Confirm** to stop the parity regeneration task.

2.7.11 Performing disk self test

This feature instructs the hard disks to start or stop short or extended disk self test (DST). The test performs a quick scan for bad sectors. To execute this function, make sure the SMART warning has been turned on. (See **2.8.1 Hard disks on page 2-56**)

Follow the steps below to start a disk self test:

1. Select **Maintenance Utilities > Disk Self Test** from the main menu.

2. Select the hard disks you want to perform the disk self test and click **DST**. Specify the following options.

Schedule	**Immediately:** The task will start immediately. **Once:** The task will start on the specified date and time. **Weekly:** The task will start on the specified day and time every week. **Monthly:** The task will start on the specified date and time every month.
Perform extended disk self test	Check this option to start an extended disk self test. Without this option, the hard disks perform short disk self test.

3. Click **Confirm** to begin testing.

To stop the DST of a hard disk, select it and click **Stop**. A confirmation prompt displays. Click **Confirm** to end the DST.

NOTE

1. Hard disks must support DST.
2. Hard disks must not be executing DST.
3. For ATA disks, the SMART must be turned on.
4. For ATA disks, if SMART is turned off during DST execution, DST will be aborted.
5. During DST execution, accessing the hard disks may lead to performance degradation.
6. For scheduling DST, the disk must be either unused, a global spare, a local spare, or a JBOD.
7. (For redundant-controller system only) The DST may not continue after failover and the following error messages may pop up (see **5.3 Redundant Controller on page 5-21** for more detailed information on failover):
   - The self-test was interrupted by the host with a hardware or software reset.
   - Self-test fail due to unknown error.

   Users can simply re-launch the DST process when encountering the above conditions. Please note that some disks may continue the DST process without any problems.

2.7.12 Array roaming

Array roaming will be activated when hard disks are moved from one slot to another or from one controller to a new controller. This ensures that the new controller can be working at all times. You can determine the way of array roaming through the Auto Array Roaming Control (See **2.7.16 Miscellaneous on page 2-55**).

When the Auto Array Roaming Control option is enabled, the configuration of the disks can be identified and restored and uncompleted tasks are automatically resumed.

Some hard disk configurations may cause conflicts when moved to a new controller. You are allowed to view group information, including the virtual disk and hard disk states, from the **Array Roaming** page.

NOTE

At the top of the page, you can select the group id and the group type (JBOD disk, disk group, or volume) for the information to be displayed. Each group type will have different columns on this page.

To import the foreign/conflict disks, click the **Import** button and specify the following options.

Target ID	Select an ID (which may be a JBOD ID, disk group ID, or volume ID) to be used after import.
Members	Select the foreign/conflict hard disks to be imported and restored the configurations. Use the arrow buttons to move the hard disks from the *Available Members* list to the *Selected Members* list.
Force to import abnormal group	Check this option to allow the import of incomplete disk groups. Without this option, only normal disk groups and volumes can be restored.

2.7.13 Array recovery

With the Array Recovery Utility (ARU), you can recover the disk groups, logical disks, and volumes. ***To perform recovery, you must fully understand the partition state of each logical disk.***

A partition of a logical disk can be one of the following states: OPTIMAL, FAULTY, , REBUILD, or UNTRUST. Each state is described as below:

- **OPTIMAL:** The partition is working and the data is valid.
- **FAULTY:** The partition is lost (the member disk is removed or faulty) and it results in a faulty logical disk. The data on the faulty partition will be still in sync with data on other partitions. The data on the faulty partition can be used after recovery.
- **BANISH:** The partition is lost (the member disk is removed or faulty) and it results in a degraded logical disk. The data on the banish partition will be out of sync with data on other partitions. The data on the banish partition can't be used after recovery.
- **REBUILD:** The member disk of the partition has been added to the logical disk, and the partition is rebuilding the data.
- **UNTRUST:** The member disk of the partition has been added to the logical disk, but the data on the partition cannot be trusted. It can become trusted if the logical disk can rebuild the data on the partition.

- **Partition state transition**

The corresponding events and state transitions of a partition are shown in the table below:

From	To
Disk is failed or removed.	
OPTIMAL	FAULTY: for faulty logical disk BANISH: for degraded logical disk
REBUILD	BANISH
UNTRUST	BANISH
Lost member disk is replaced by a new disk for disk rebuilding.	
FAULTY	UNTRUST (The logical disk is not recoverable.)
BANISH	UNTRUST (and later to REBUILD)
Lost member disk is restored to a disk group by the ARU.	
FAULTY	OPTIMAL
BANISH	UNTRUST (and later to REBUILD)
Force to recover a logical disk by the ARU.	
UNTRUST	OPTIMAL
Force to recover a logical disk by the ARU.	
UNTRUST	REBUILD
The partition completes data rebuilding.	
REBUILD	OPTIMAL

Table 2-12 State transition

Before logical disk recovery, make sure the following:

- There are enough hard disks in the disk group.
- No background tasks in progress, such as disk rebuilding or RAID reconfiguration.
- No reconfiguration tasks are performed by the faulty logical disk.

- **Start a recovery**

When there are any hard disk conflicts, there might be faulty disk groups, logical disks, or volumes on your controller. You can perform DG recovery to restore lost member disks to a disk group. The faulty logical disks on the disk group are recovered automatically when the disk group is recovered.

To perform a disk group recovery, do the following:

1. Select **Maintenance Utilities > Array Recovery** from the main menu.

2. Select **DG** from the Recovery Type drop-down menu.
3. Select a disk group, and click **Recover**.
4. The **Restore the Array** window displays. Select the original member disks to restore.

NOTE

1. If a non-member disk is selected, check the **Force to recover disk** option and specify the Disk Member Index. Make sure the recovery index is correct.
2. To reduce the possibility of data loss, ensure that the recovery order is correct when the **Force to recover disk** option is chosen.

5. Click **Apply** and a confirmation prompt displays. Click **Confirm**.
6. The disk group recovery starts. Rebuilding will also start for degraded logical disks on a disk group.

If the logical disk is not recovered automatically after disk group recovery, perform logical disk recovery. After logical disks are restored, you can perform the volume recovery to restore the lost member logical disks to a volume.

2.7.14 Schedule task

The DG reconfiguration, LD reconfiguration, disk cloning, disk scrubbing, and DST scheduled tasks are listed in the **Schedule Task** section. When the scheduled date and time is met, the controller will start the specified tasks.

NOTE

The controller will try to launch commands according to the schedule. However, if the command cannot be executed at that moment, the controller will not retry.

To cancel a scheduled task, select it and click **Delete**. A confirmation prompt displays. Click **Confirm** to delete the selected task.

2.7.15 Cache Configurations

In this section, you can configure the following settings to the controller. The settings of Cache Unit Size, Auto Array Roaming Control, and Write Log Control will take effect after you restart the RAID subsystem.

Cache Unit Size (KB): 4 / 8/ 16 / 32 / 64 / 128 (default)

The cache unit size must be smaller or equal to the minimum stripe size of existing logical disks.

Read Ahead Expire Control (1/100 second):55 (default)

Specify the read ahead expire control in 1/100 seconds.The range is from 10 to 1000.

Write Cache Periodic Flush (second): 5 (default)

Specify the period in seconds to periodically flush the write cache. If 0 is specified, periodic cache flushing is disabled. The range is from 0 to 999.

Write Cache Flush Ratio (%): 45 (default)

Specify the dirty write buffer watermark. When the specified percentage is reached, the system will start to flush the write buffers immediately. The range is from 1% to 100%.

Mirrored Write Cache Control: On (default) **/ Off**

This option is only available on the redundant-controller system. If this option is enabled, all written data from hosts will be mirrored to the peer controller.

NOTE

Mirrored Write Cache will improve the write performance, but it will cause data loss when a controller fails. Do not disable it if you need dual active-active controller configuration.

2.7.16 Miscellaneous

Auto Spare Control: On (default) **/ Off**

If this option is enabled, and there is no global spare disk, unused hard disks are used for rebuilding. If there are multiple unused disks, the disk with the lowest hard disk identifier will be used.

Spare Restore Control: On / Off (default)

If this option is enabled, the controller will restore the data from the spare disk to a new replacement disk when inserted. This allows the user to keep the same member disks as original.

Auto Array Roaming Control: On / Off (default)

On: Enable imported foreign hard disks when the controller is started. Foreign hard disk configurations are also restored.

Off: Disable imported foreign hard disks when the controller is started.

NOTE

Hard disks with configurations that conflict with controller configurations are not imported and enter conflict state.

On-line Array Roaming Control: On / Off (default)

On: The controller will try to keep the disk in the foreign state if hard disk contains valid meta-data. However, if the disk fails to import successfully, it will enter the conflict state.

Off: All on-line installed disks are perceived as new disks and enter unused state. Meta-data on the disk is cleared and reset.

Write Log Control: On (default) **/ Off**

The consistency of parity and data might not be retained because of improper shutdown of the controller. This option enables or disables write logging for parity consistency recovery.

NOTE

1. Enabling write logging will cause slight performance degradation.
2. Write logging is only effective to logical disks with parity-based RAID levels.
3. To guarantee the consistency of data and parity by write logging, the on-disk cache must be turned off.

Meta-data Update Frequency: Low (default) **/ Medium / High**

This option specifies the frequency to update the progress of background tasks, except reconfiguration tasks.

Task Notify: On / Off (default)

Select this option to enable or disable the event notification when the background task is completed to a specified percentage. The range is from 1% to 99%.

2.8 Hardware Configurations

2.8.1 Hard disks

In this section, you can configure the following settings to all hard disks.

Utilities Task Priority: Low (default) **/ Medium / High**

This option determines the priority of the background tasks for utilities of all hard disks not belonging to any disk group, such as scrubbing and cloning.

SMART Warning: On / Off (default)

This option is only for SMART function supported hard disks. The SMART function serves as a device status monitor.

Period of SMART Polling (minute): 60 (default)

This option is only available when the SMART warning is turned on. Specify the period in minutes to poll the SMART status from hard disks periodically.

SMART Action: Alert (default) **/ Clone**

This option is only available when the SMART warning is turned on. The controller will alert you or start disk cloning when a disk reports a SMART warning.

Disk IO: timeout after 30 (default) **sec(s) and retry 1** (default) **time(s)**

Timeout value (in unit of seconds): If a hard disk does not respond to a command within this time, the controller will reset and reinitialize the hard disk, and retry the command. The possible values are 1 to 60.

Retry times: Specify the number of retries when a disk IO command fails. The possible values are 0 to 8.

Transfer Speed: Auto (default) **/ 1.5GB / 3GB**

This option specifies the transfer speed of a hard disk. When **Auto** is specified, the transfer speed is determined by the controller according to the best transfer mode supported by the installed hard disks.The option is available only for RAID controller with SATA disk interface.

Bad Block Alert: On / Off (default)

This option enables or disables event alerts for bad block reallocation. After selecting **On**, four blank fields are displayed for you to specify the percentages of reserved bad block reallocation space. The default values are 20, 40, 60, and 80.

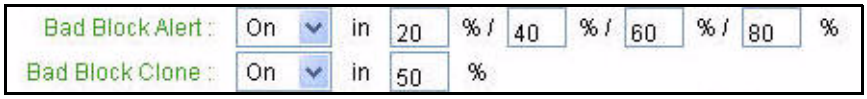


Figure 2-23 Specify the percentage for Bad Block Alert

NOTE

1. Latter percentages must be larger than the former percentages.
2. Percentages must be integers between 1 and 100.

Bad Block Clone: On / Off (default)

This option enables or disables disk cloning for bad block reallocation. After selecting **On**, a blank field is displayed for you to specify the percentage of reserved bad block reallocation space. When the specified space is reached, disk cloning will be started. The default value is 50.

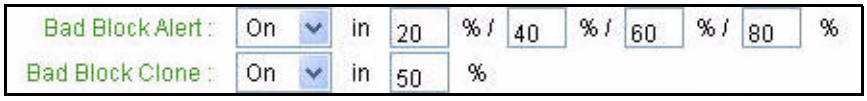


Figure 2-24 Specify the percentage for Bad Block Clone

NOTE

1. Percentages must be integers between 1 and 100.
2. Cloning can only be started when there are local or global spare disks.

Bad Block Retry: On (default) **/ Off**

Select this option to enable or disable retrying when bad block reallocation fails.

IO Queue: On (default) **/ Off**

Select this option to enable or disable *Negative Command Queue (NCQ)*, which enhances hard disk read performance.The option is available only for RAID controller with SATA disk interface.

Disk Standby Mode: On / Off (default)

Select this option to enable or disable disk standby mode after a period of host inactivity.

Disk Access Delay Time (second): 15 (default)

Specify the delay time before the controller tries to access the hard disks after power-on. The range is between 15 and 75.

Delay Time When Boot-Up (second): 40 (default)

Specify the delay time before the controller automatically restarts. The range is between 20 and 80.

CAUTION

The boot-up delay time must be longer than the disk access delay time plus 5 seconds.

2.8.2 FC/SAS/SCSI ports

This shows information about FC/SAS/SCSI ports. For FC ports including Controller Failover Mode (for redundant controller only), each port's ID, name, WWN, Hard loop ID, connection mode (private loop, public loop, or point-to-point), and data rate. For SAS ports including each port's ID, name and SAS address. For SCSI ports including each port's ID, name,

default SCSI ID and data rate. To change the settings, follow the instructions given below:

NOTE

In redundant-controller systems, the four FC ports are given identifiers fcpa1, fcpa2, fcpb1, and fcpb2 to identify the corresponding port positions located on each controller.

1. Select an FC/SAS/SCSI port and click **Modify** to open the configurations window.
2. Specify the following options.

Controller Failover Mode	(For FC port with redundant controller only) **Multipath IO:** This mode allows the host computer to access the RAID system over multiple paths. To use this mode, Pathguard needs to be installed. See **5.1 Multi-Path IO Solutions** for more information. **Multiple-ID:** This function requires the use of fiber switch. When you select this function, only simple method is available for storage provisioning. See **5.2 Multiple ID solutions** for more information.
Name	Type a name associated with each FC/SAS/SCSI port. The maximum name length is 15 bytes. For SAS ports please jump to step 4 after setting name.
Hard Loop ID	Select a fixed loop ID for each FC port from the drop-down menu. To disable hard loop ID, select **Auto**. The loop ID is automatically determined during loop initialization procedure.
Connection Mode	**Auto:** The controller will determine the connection mode automatically. **Arbitration loop:** This is a link that connects all the storages with the host, which enables data transferring. **Fabric:** This is a point to point connection mode without a switch.
Default SCSI ID	(For SCSI port) Select a fixed SCSI ID for each SCSI port from the drop-down menu. The ID range is from 0 to 15.

Data Rate	**Auto / 1GB / 2GB / 4GB** Select a preferred data rate for an FC port or all FC ports. (For SCSI port) **Async / Fast / Fastwide / Ultra / Ultrawide / Ultra2 / Ultra2wide / Ultra3 / Ultra320** Select a preferred data rate for an SCSI port or all SCSI ports.The default setting is Ultra320.

3. Check the '**Apply connection mode and data rate to all FC ports**' option if necessary.
   Check the '**Apply data rate to all SCSI ports**' option if necessary (SCSI port).
4. Click **Apply** and the 'Restart to Apply' prompt box appears. Click **Restart** to restart the controller immediately, or **OK** to restart later.
5. All settings except FC/SAS/SCSI port name are effective after you reconnect the controller.

- Setting FC Worldwide Node Name

The default worldwide port name (WWPN) of each FC port should be different. The assignment of worldwide node names (WWNN) to all FC ports help the RAID system recognize all the FC ports with the same WWPN as one device.

To set FC worldwide node name, click the **WWNN** button. Then select **Distinct** to use different FC WWPNs, or **Identical** to synchronize all FC ports using the same WWNN. Click **Apply** to save. The WWPN of all FC ports will be synchronized the next time you start the RAID system.

2.8.3 COM port

In this section, you can configure the terminal settings on the COM port as instructed below. Select Terminal port, and click **Modify** to open the configurations window.

- Terminal port

The terminal port serves as one of the mechanisms to manage the controller on-site. The configurations for the terminal ports are baud rate, stop bit, data bit, parity check, and flow control.

To change the settings, specify the following options:

Baud Rate: 2400 / 4800 / 9600 / 19200 / 38400 / 57600 / 115200 (default)
Stop Bit: 1(default) **/ 2**
Data Bit: 7 / 8 (default)

Parity Check: None (default) **/ Even / Odd**

Flow Control: None (default) **/ HW**

NOTE

In a redundant-controller system, the two controllers use the same configuration for the terminal port.

2.9 Event Management

Event Management enables or disables event notifications. When an event is detected, the controller will alert you by the specified notification methods. All the events will be recorded in the controller. You are allowed to erase and download the log, and send a test email of events.

2.9.1 Setting up the SMTP

The controller can notify you when an event occurs by sending a mail to the specified user account. Specify the following options for event configurations.

Notify State: On / Off (default)

This option enables or disables the SMTP event notifications.

Mail Subject: RAID system event notification (default)

Enter the mail subject. The maximum length is 31 bytes.

Mail Content: By default, there is no content.

Enter the mail content. The maximum length is 47 bytes.

Mail Retry Period (minute): 10 (default)

Specify the period of time in minutes to retry sending event notification mail. The range is from 10 to 60.

Mail Delay Time (second): 10 (default)

Specify the delay time in seconds to send out multiple events in one mail. This helps to reduce the number of mails. The range is from 5 to 60.

Add Event Receivers

You can add a maximum of three mail recipients. Click **Add** to set the receiver ID, mail receiver address, and the corresponding severity level.

Remove Event Receivers

Select the mail recipient(s) you want to delete and click **Remove**. The selected mail recipients are deleted.

Modify Event Receivers

Select a mail recipient you want to change for its mail address and the event severity level. Click **Modify** to enter the settings screen.

2.9.2 Setting up the SNMP

SNMP (Simple Network Management Protocol) is a widely used protocol based on TCP/IP for monitoring the health of network-attached equipments. The RAID controller is equipped with an embedded SNMP Agent to support SNMP-based monitoring. You can use SNMP applications (SNMP v1 or v2c-compliant) at remote computers to get event notification by SNMP traps and watch the status of a RAID system. Please contact your RAID system provider to get the MIB (Management Information Base) file and import the MIB file to your SNMP manager before enabling this feature.

Notify State: On / Off (default)

This option enables or disables the SNMP trap event notifications.

SNMP Agent State: On / Off (default)

This option enables or disables the SNMP Agent for status watching.

Port :161 (default)

Set up the port by which the SNMP Agent receives the status retrieval commands from SNMP applications.

Community Name: public(default)

Set up the community name as the authentication string between the SNMP Agent and SNMP applications.

Add SNMP Event Receivers Servers

You can have up to three SNMP servers to receive SNMP event notification packets. Click **Add** to choose a Server ID, and set its SNMP server address, port, and the corresponding protocol version, community name, and severity level.

Server ID: 0 / 1 / 2

Select a server ID from the drop-down menu.

Server Address: IP Address / Domain Name

Set up the IP address or the domain name of the SNMP server.

Port : 162 (default)

Set up the port on which the SNMP server receives SNMP event notification packets.

SNMP Version: v1 (default) **/ v2c**

Specify the SNMP version and the event notification type. Choosing v1 for SNMP trap event notification and choosing v2c for SNMP INFORM event notification. Traps are unreliable because the receiver does not send any acknowledgment when it receives a trap. An SNMP manager that receives an INFORM request acknowledges the message with an SNMP response PDU. However, some SNMP applications may not support SNMPv2c.

Community Name : public (default)

Set up the community name in the event notification packets such that your SNMP applications can know how to process it.

Severity Level: Notice (default) **/ Warning / Error / Fatal**

Events with a severity level higher than the specified one will be sent via SNMP traps.

Remove SNMP Servers

Select the SNMP server(s) you want to delete and click **Remove**. The selected SNMP server(s) are deleted.

Modify SNMP Servers

Select the SNMP you want to change for the settings and then click **Modify** to enter the settings screen.

Send a Test SNMP Trap

Select the SNMP server(s) to which a test SNMP trap will be sent, and click **SNMP**. The test SNMP trap will contain message "This trap is for testing purpose only."

NOTE

In a redundant-controller system, both controllers send out SNMP event notification packets for one event.

- **SNMP MIB Definition**

A Management Information Base (MIB) is a collection of information that is organized hierarchically.MIBs are accessed using a network-management protocol such as SNMP. They are comprised of managed objects and are identified by object identifiers.If a vendor(RAID controller) wishes to include additional device information that is not specified in a standard MIB, then that is usually done through MIB extensions.

SNMP MIB Installation (Ex. iReasoning MIB Browser)

1. Installing the SNMP MIB Manager software on the client server.
2. Importing a copy of the MIB file in a directory which is accessible to the management application.
   (MIBs Sotre Location:\iReasoning\mibbrowser\mibs)
3. Compiling the MIB description file with the management application.
4. Set Agent's Charset to IS0-8859-1 (Choose Tools > Options > General).

NOTE

Before the manager application accesses the RAID controller, user needs to integrate the MIB into the management application's database of events and status indicator codes. This process is known as compiling the MIB into the application. This process is highly vendor-specific and should be well-covered in the User's Guide of your SNMP application. Ensure the compilation process successfully integrates the contents of the "**ACS-RAID-MIB.MIB**" file into the traps database. Each SNMP MIB application's have some different.For more information refer to management application's user manual

SNMP MIB Operation (Ex. iReasoning MIB Browser)

5. Set RAID controller IP address of SNMP managment application.
6. Choose ACS-RAID-MIB on MIB tree,and then expand the tree to choose xxxx Table component, execute Ctrl+T to open Table View.

2.9.3 Event logs

When the state of a logical or physical component in the controller changes, such as failure of hard disks or completion of a background task, an event occurs.

Events are classified into different severity levels. You can view the events according to the different categories. Specify the severity level at the top of the page.

Events are listed in the event log from newer to older. The events contain the following information:

1. Sequence number
2. Severity level of the event
3. Date and time when the event is occurred
4. The message text of the event, its associated parameters, and event identifier.

For the complete list of event messages, refer to **" Appendix D: Event Log Messages on page D-1"**

Erase Event Log

To clear all the records in the event log, click **Erase**. A confirmation prompt displays. Click **Confirm** and all records will be erased.

Download Event Log

To download all the records in the event log, click **Download**. Select a file type from the drop-down menu, and click **Apply**.

File Type	**.csv (excel-readable) / .txt (human-readable) / .bin (for system suppliers)** Click on the link in the following pop-up message and the **File Download** window displays. Select **Save** and the download task begins. If **.txt** is specified as the file type, right click the link to save the file.

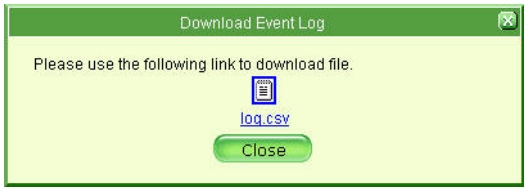


Figure 2-25 Event log download message

Click **Close** to close the window.

NOTE

The event log file stores details of controller activity. In the case of malfunction, this data can be analysed by the user to determine the cause(s).

Record Event Log

Click **Configure** and specify the **Lowest severity of events** option for the events you want to record on NVRAM. The events with severity levels higher than the specified one will be recorded. The default severity level is *info*, which means events of all severity levels will be recorded.

Send a Test Mail

Click **Configure** and specify the **Severity of testing event** option to send a test mail. A testing event record will be generated according to the selected severity level. This helps users to test the event logging and notifications setup.

NOTE

Before sending out the test mail, you need to turn on the event notification and specify the event receivers. (Refer to **2.9.1 Setting up the SMTP on page 2-61**.)

2.9.4 UPS

The **UPS Control** option enables or disables the UPS function when the controller is started. When this option is set to **On**, the controller will automatically detect if the UPS is connected or not.

To configure the UPS settings, do the following:

1. Select **Event management > UPS** from the main menu, you can view the UPS information, status, and battery status here.
2. Click **Configure** and specify the following options.

Change Date (YYYY/MM/DD)	This option resets the latest battery replacement date.
Delay Shutdown (seconds)	**90 / 180 / 270 / 360 / 450 / 540 / 630** When a power failure occurs and the UPS battery charge is below the normal range, the UPS will power down after the specified delay time.
Delay Boot (seconds)	**0 / 60 / 120 / 180 / 240 / 300 / 360 / 420** The UPS automatically powers on after the specified delay time. This avoids branch circuit overload when AC power returns.
Low Battery Threshold (seconds)	**120 / 300 / 480 / 660 / 840 / 1020 / 1200 / 1380** This option notifies the user that the UPS battery is low, with the specified remaining seconds.
Change Restart Percentage	**0 / 15 / 30 / 45 / 60 / 75 / 90** After the AC power returns, the UPS does not power on until the battery charge reaches the specified capacity.

3. Click **Apply** to confirm the current settings.

NOTE

1. The values from each drop-down menu may be different according to the UPS connected.
2. Currently the controller only support and communicate with Smart-UPS function **APC** (American Power Conversion Corp.) UPS. Please check detail **http://www.apc.com/**.

2.9.5 Miscellaneous

Beeper Control: On (default) **/ Off / Mute**

This option controls the controller's beeper.

On: The beeper sounds during exceptional conditions or when background tasks make progress. By default, the beeper is on.

Off: The beeper is quiet all the time.

Mute: This temporarily mutes the beeper, but it beeps again if exceptional conditions still exist.

Auto Write-Through Cache

This option enables or disables the auto write-through function for the following four types of events.

1. Controller Failure
2. Battery Backup Module Failure
3. Power Supply Unit Failure
4. Fan Failure
5. UPS Failure

When events are detected with a specified type, both the cache on the controller and disk will be automatically set as write-through. After the failure or warning condition is removed, the cache settings will be restored to your original configuration.

Path Failover Alert Delay (min): 5 (default)

When a path failover occurs, the controller will send out warning events to notify users after the specified delay time (in minutes). The range is between 0 and 60.

To make the settings effective, click **Apply**.

2.10 System Management

2.10.1 Restoring to factory settings

To clear the NVRAM or hard disk configurations, do the following:

1. Select the **"Erase configurations on NVRAM"** or the **"Erase configurations on HDD(s)"** option to clear all configurations made on NVRAM or hard disks.
2. When the **"Erase configurations on HDD(s)"** option is selected, specify the hard disks or a hard disk to clear the configurations on it.

3. Click the **Apply** button, and the erase configuration message appears. Click **Confirm** to restore factory default values.

NOTE

1. The **"Erase configurations on HDD(s)"** option will be available only when hard disks are in foreign, conflict, or unknown state.
2. After the erase command is applied to NVRAM, the controller will restart immediately.

2.10.2 NVRAM configuration

The controller's configurations are stored in either NVRAM or hard disk(s) depending on configuration types. The following options allows you to manage the configuration data.

Save the NVRAM configuration to HDD(s)

Specify this option to save the NVRAM configuration data to a hard disk or all hard disks.

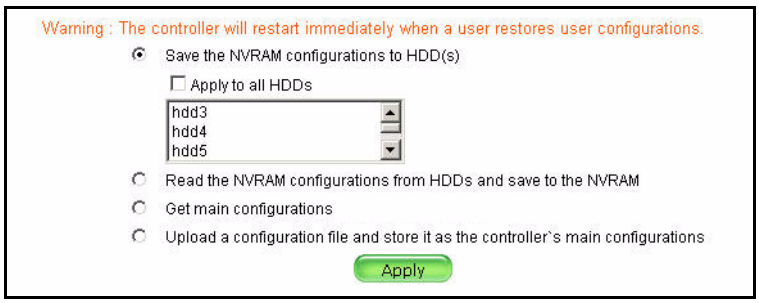

Warning : The controller will restart immediately when a user restores user configurations.
Save the NVRAM configurations to HDD(s)
Apply to all HDDs
hdd3
hdd4
hdd5
Read the NVRAM configurations from HDDs and save to the NVRAM
Get main configurations
Upload a configuration file and store it as the controller's main configurations
Apply

Figure 2-26 Options in the Configurations screen-1 (System Management menu)

Read the NVRAM configuration on hard disks and save to NVRAM

Specify this option to read the NVRAM configuration data on the specified hard disk and save to NVRAM.

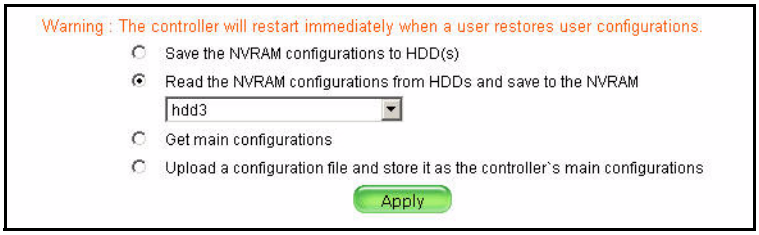

Warning : The controller will restart immediately when a user restores user configurations.
Save the NVRAM configurations to HDD(s)
Read the NVRAM configurations from HDDs and save to the NVRAM
hdd3
Get main configurations
Upload a configuration file and store it as the controller`s main configurations
Apply

Figure 2-27 Options in the Configurations screen-2 (System Management menu)

NOTE

This option will be available when on-line hard disks exist. Therefore, only on-line hard disks will be displayed in the list box.

Get main configurations

Specify this option to save the NVRAM configuration data to a file. The following three options are available:

.bin (for user to backup configuration): The configuration data is saved as config.bin.

.html (human-readable): The configuration data is saved as config.html.

.html (to send human-readable mail): The configuration data is saved as config.html, which is then sent to a specified mail receiver. When this option is selected, enter a mail address for the receiver.

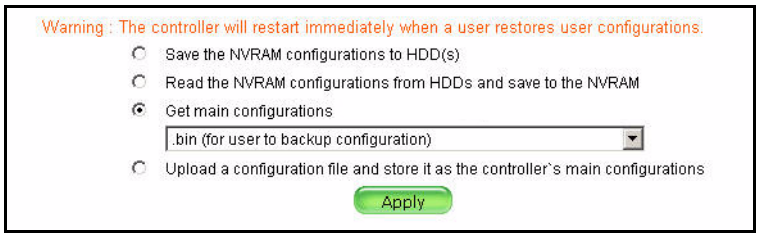

Warning : The controller will restart immediately when a user restores user configurations.
Save the NVRAM configurations to HDD(s)
Read the NVRAM configurations from HDDs and save to the NVRAM
Get main configurations
.bin (for user to backup configuration)
Upload a configuration file and store it as the controller`s main configurations
Apply

Figure 2-28 Options in the Configurations screen-3 (System Management menu)

Upload a file and store it as the controller's main configurations

Specify this option to upload a configuration file and store it on NVRAM.

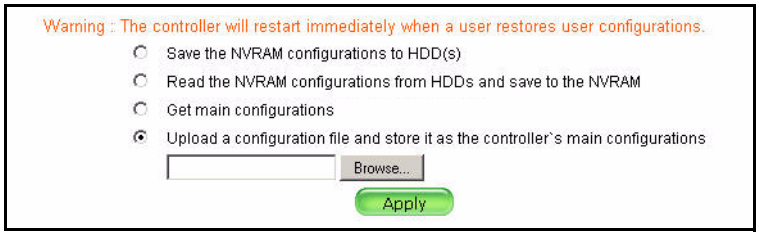

Warning : The controller will restart immediately when a user restores user configurations.
Save the NVRAM configurations to HDD(s)
Read the NVRAM configurations from HDDs and save to the NVRAM
Get main configurations
Upload a configuration file and store it as the controller`s main configurations
Browse...
Apply

Figure 2-29 Options in the Configurations screen-4 (System Management menu)

2.10.3 Setting up the network

The network interface serves as one of the methods to manage the controller. There are two network types, static and DHCP.

To set up the network, do the following:

1. Select **System Management > Network** from the main menu.
2. (For the redundant-controller system only) From the Controller drop-down menu, select the desired controller for the following network settings to apply.
3. From the Assignment Method drop-down menu, select either static, DHCP or DHCP+APIPA.
   - If you select the static method, assign the IP address, network mask, gateway, and DNS Server to the network.
   - If you select the DHCP method, assign the DNS server address.
   - If you select the DHCP+APIPA method, assign the DNS server address.
4. Click **Apply**, and the settings are effective immediately.

NOTE

If DHCP is selected for the network, you need to close the GUI and use the new IP for the connection.

NOTE

APIPA stands for Automatic Private IP Addressing. If DHCP+APIPA is selected and the controller cannot get response from DHCP servers on the network, the controller will choose an unused IP adress in the private address space between 169.254.0.0 and 169.254.255.255 (address conflict is avoided by probing the network).

Reset SMTP server

Select a server you want to clear the SMTP configurations from, and click **Reset**.

Configure or Modify SMTP server

Select a server you want to configure and click **Modify**. The configurations window opens. Enter the information for the following options.

Server Address	Set the SMTP server address.
Port	Enter the SMTP port for the outgoing mails. Check with your ISP provider for the port number to use. By default, the port is set to 0.
SSL Setting	Enable or disable the SMTP server to use secure connection.
Sender Account	Set the account to be used on the SMTP server.
Authentication	Turn the authentication on or off for the SMTP server.
Password	Set the password of the account on the SMTP server.
Name	Set the name to be shown in the sender field. If this option is not set, the sender account on the SMTP will be used.

Test SMTP server

Select a server and click **Test SMTP** to ensure the SMTP server is correctly configured. The **Send Test Mail** window displays. Enter an email address for testing.

NOTE

The primary and secondary server must not be the same SMTP server and sender.

2.10.4 System Time

- **Setting up the Time**

Time is required for the controller to record events and to schedule maintenance tasks. There are two time modes for selection, static and NTP settings.

For network settings, do the following:

1. Select **System Management > Time** from the main menu.
2. From the Time Mode drop-down menu, select either static or NTP.
   - If you select the static mode, specify the date and time. The data and time is set in form as *MM/DD/YY* and *hh/mm*.

- If you select the NTP mode, specify the IP address or the domain name of the NTP server. The NTP server automatically synchronizes the controller clock at 23:59 every day.

3. Click **Apply**, and the settings are effective immediately.

- **Setting up the Time-Zone**

1. Select **System Management > Time** from the main menu.
2. From the Time-Zone Mode drop-down menu, select location of country.
3. From the DST(Daylight saving time) Status Mode drop-down menu, select On/Off(default).
4. Click **Apply**, and the settings are effective immediately.

NOTE

If the NTP server is located outside your LAN, make sure the gateway and domain name server is configured properly for the RAID controller to conect to the NTP server.

2.10.5 Security control

The settings in the **Security** page allows you to change the password and login related settings.

- **User setting**

To change the password of a specified user, do the following:

1. Specify either Administrator or User from the **Specified User** drop-down menu.
2. Check the "**Change Password**" checkbox, and a pull-down menu appears. Fill in the passwords in each field.
3. If you want to enable or disable password checking before login, specify the options from the **Password Check** drop-down menu.

- **Global Setting**

To enable or disable the auto logout function, select either **On** or **Off** from the **Auto Logout** drop-down menu. By default, the auto logout time is 10 minutes.

Set the **Password Reminding Mail** option to **On** to enable the controller to send out a password reminding email when users forget their password. An email account is also required.

- **SSL Setting**

A secure connection is always required to login to the GUI; therefore, 'SSL Forced' is enabled by default and users are forced to connect to the system via HTTPS.

To disable forced SSL encryption, select either **On** or **Off** from the **SSL Forced** drop-down menu.

When all the settings are complete, click **Apply** to make them effective immediately.

2.10.6 System information

To view system information and controller information, select **System Management > System Information** from the main menu. You will see the following details.

System Information	• System Name • Vendor Name • Model Name • Product Revision • Product Serial Number
Controller Information	• Controller ID • RAM Size (MB) • Serial Number • Controller Name

NOTE

When the redundant-controller system is in use, both controllers (ctla and ctlb) information will be shown on the screen.

2.10.7 Battery backup module

To view battery information, ensure that a battery backup module is connected. Select **System Management > Battery Backup Module** from the main menu, and the battery information will be displayed in this page. Use the BBM Control option to turn on or off the BBM icon shown in the Monitor mode.

Battery Information	• State • Remaining Capacity • Voltage (V) • Temperature (°C/°F) • Non-critical Temperature (°C/°F) • Critical Temperature (°C/°F)

NOTE

When the redundant-controller system is in use, both controllers' (ctla and ctlb) battery information will be shown on the screen.

2.10.8 Update system firmware, boot code and external enclosure F/W

To update the system's firmware, boot code and external enclosure firmware, do the following:

1. Select **System Management > Firmware Update** from the main menu.
2. Specify the firmware type; the current firmware, boot code version and external enclosure amount will be also displayed on-screen.
   - For firmware update, click on the System firmware radio button.
   - For boot code update, click on the Boot Code radio button.
   - For external enclosure firmware update, click on the External enclosure firmware radio button.and to choose enclosure ID number.
3. Click **Browse** to select an update file.
4. Click **Apply**, and a confirmation prompt displays. Click **Confirm** to continue.
5. The controller will immediately start the update task in the background.

NOTE

1. Contact your RAID system supplier before updating the firmware. DO NOT udpate the firmware unless you fully understand what a version of firmware will do. One of the general rules is not to update the firmware using an older version. Otherwise, the system might not work properly.
2. When updating the firmware, boot code and external enclosure firmware, do not perform any actions in GUI or power off the controller.
3. For external enclosure firmware option, you can check the 'Apply' to all external enclosure' option to apply the updating to all external enclosure at the same times.
4. After updating the firmware for external enclosures, it requires to restart both the controllers for the RAID system and all external enclosures.
5. The RAID controller supports redundant flash chip for system firmware. Primary chips will be updated first and the secondary chips later. Wait for the completion of firmware update of both chips.
6. The redundant-controller RAID system supports uninterruptable firmware update (but it depends on the compatibility of your running and new firmware, contact your system supplier to know the compatibility). After updating the firmware to the flash chip one both controllers, one controller will be restarted first and the other controller will be restarted later. During the restart, the controller will take over the peer controller. However, for updating the firmware of external enclosures, rebooting is still needed.

2.10.9 Restart or halt the controller

When you want to turn the RAID system off, you must go through a regular shutdown procedure. Always follow the steps below to instruct the controller restart or halt before powering off the RAID system.

1. Select **System Management > Restart/Halt** from the main menu.
2. (For redundant-controller system only) From the Controller ID drop-down menu, specify whether you want to restart or halt **ctla**, **ctlb**, or **Both Controllers**.
3. From the Action drop-down menu, select **Restart** or **Halt**.
4. Once any external SAS JBOD enclosure is connected, the '**Apply to all external enclosures**' checkbox will be displayed. Check this checkbox to restart or halt all the enclosures at the same time.
5. Click **Apply**.
   - When **Restart** is selected, the controller automatically restarts. Click **Reconnect** when boot up is complete.
   - When **Halt** is selected, a confirmation prompt displays. Click **Confirm**, close the GUI, and power off the RAID system.

2.10.10 Miscellaneous

Select **System Management > Miscellaneous** from the main menu, and the following settings become available for your controller.

Enclosure Polling Period (second): Disabled (default)**/1/2/5/10/30/60**

(This option is only available for the controller equipped with an expansion port.)

By specifying the polling interval, the controller polls the external enclosure to acquire its status periodically. When disabled, the controller cannot obtain the status of the enclosures.

GUI Refresh Rate (second): 5 (default)

By default, the GUI refreshes itself every 5 seconds. You can specify a new refresh rate. The range is from 2 to 15.

Memory Testing When Boot-Up: On(default)**/Off**

Select this option to enable or disable memory testing when controller boot-up.

Management Device for In-band API: Off(default)**/LUN ID(0~127)**

Select this option to enable or assign LUN ID when user want to use In-band API Utility.

NOTE

Faster GUI refresh rates may degrade the performance of controller.

To make the settings effective, click **Apply**.

2.11 Performance Management

2.11.1 Hard disks

This feature allows you to enable, disable, or reset disk IO logging for all hard disks.

When hard disk IO logging is enabled, the following data will be displayed. You can press the **Reset** button to clear all statistics except outstanding IO and disk utilization to zero.

Category	Display
HDD ID	Hard disk identifier
Read Command (sector)	The number of read commands executed since the disk was powered on
	The accumulated transfer size of read commands since the disk was powered on
Write Command (sector)	The number of write commands executed since the disk was powered on
	The accumulated transfer size of write commands since the disk was powered on
Response Time (ms)	The average command response time since the disk was powered on
	The maximum command response time since the disk was powered on
Outstanding IO	The number of current outstanding IO in the disk
	The number of current outstanding IO in the controller's IO scheduler queue
Disk Utilization	The disk utilization in the last second
	The disk utilization in the last five seconds

NOTE

When the redundant-controller system is in use, all the statistics information of the hard disks in both controllers (Controller A and B) will be displayed on the screen.

2.11.2 Cache

This feature allows you to enable, disable, or reset buffer cache IO logging.

When cache IO logging is enabled, select the cache type (volume, logical disk, or JBOD disk) to be displayed from the drop-down menu. The

following IO statistics will be displayed. You can press the **Reset** button to clear all statistics except dirty buffer and clean buffer to zero.

Category	Display
ID	Cache identifier
Read Command (sector)	The number of read commands executed since the disk was powered on
	The accumulated transfer size of read commands since the disk was powered on
Write Command (sector)	The number of write commands executed since the disk was powered on
	The accumulated transfer size of write commands since the disk was powered on
Read Cache Hit	The number of cache hits by read commands since the system was powered on
Merged Write	The number of merged writes (write hits) since the system was powered on
Dirty Buffer	The number of dirty buffers in the cache at present
Clean Buffer	The number of clean buffers in the cache at present

2.11.3 LUN

This feature allows you to enable, disable, or reset LUN IO logging.

When LUN IO logging is enabled, the following IO statistics of a LUN (depending on the storage presentation method selected) will be displayed. You can press the **Reset** button to clear all statistics except outstanding IO to zero.

Category	Display
ID	Storage group and LUN identifier
Read Command (sector)	The number of read commands executed since the disk was powered on
	The accumulated transfer size of read commands since the disk was powered on
Write Command (sector)	The number of write commands executed since the disk was powered on
	The accumulated transfer size of write commands since the disk was powered on
Response Time (ms)	The average command response time since the disk was powered on
	The maximum command response time since the disk was powered on
Outstanding IO	The number of current outstanding IO

NOTE

When the redundant-controller system is in use, all the LUN statistics information in both controllers (Controller A and B) will be displayed on the screen.

Click to see a complete list of LUN information. You will see the specified LUN ID and its histogram output in the following sectors.

The histogram output shows the sizes that the read and write commands return.

- LUN ID
- 1 Sector
- 2 Sector
- 4 Sector
- 8 Sector
- 16 Sector
- 32 Sector
- 64 Sector
- 128 Sector
- 256 Sector
- 512 Sector

2.11.4 Storage port

This feature allows you to enable, disable, or reset storage port IO logging.

When storage port IO logging is enabled, the following statistics of a FC ports or SAS port will be displayed. You can press the **Reset** button to clear all statistics to zero.

Category	Display
HTP ID	FC/SAS port identifier
Link Failure Count	The value of the LINK FAILURE COUNT field of the Link Error Status Block for the port
Loss of Sync Count	The value of the LOSS-OF-SYNCHRONIZATION COUNT field of the Link Error Status Block for the port
Loss of Signal Count	The value of the LOSS-OF-SIGNAL COUNT field of the Link Error Status Block for the port
Invalid TX Word Count	The value of the INVALID TRANSMISSION WORD field of the Link Error Status Block for the port
Invalid CRC Count	The value of the INVALID CRC COUNT field of the Link Error Status Block for the port

Click to see a complete list of storage port information. You will see the following details.

- HTP ID
- Primitives Sequence Protocol Error Count
- Second since last reset
- TX/RX Frame
- TX/RX Word
- LIP Count
- NOS Count
- Error Frame
- Dumped Frame

NOTE

The information displayed is dependent on the installed FC chip. Some chips do not support the provision of all storage port information.

Chapter 3: Using the LCD Console

3.1 Starting LCD Manipulation

The RAID system has a front LCD panel which supports a quick configuration and RAID monitoring. You can use the four buttons on the LCD panel to manipulate the LCD configuration utility. Each state and display sequence is illustrated as below:

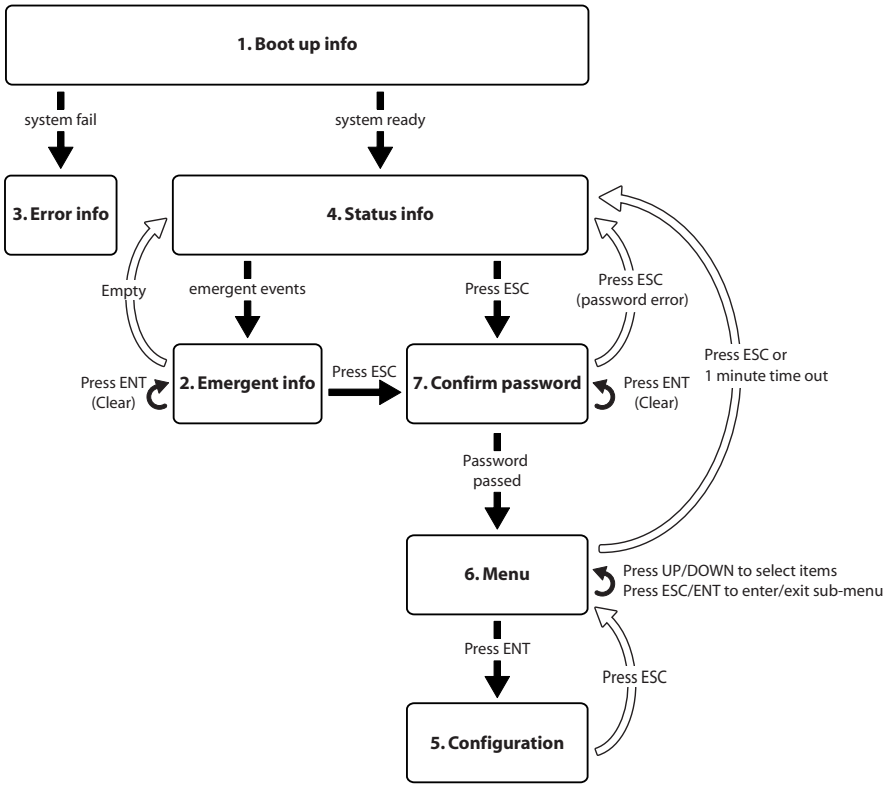


Figure 3-1 LCD manipulation procedure

Once the RAID system is powered on, the booting information starts to display on the LCD panel. If the system is ready, status messages are displayed sequentially. If not, error messages are displayed and the system is halted. See the details of status and emergent messages in the following section ***3.2 LCD Messages***.

3.1.1 Confirm password

To enter the menu, a password may be required depending on your settings. The default password is "0000". Use the buttons for password input. See the use of buttons as below.

UP/DOWN: Select the numbers 0 to 9, characters "a" to "z".

ENT: Enter the selected character, or confirm the password if no character is selected.

ESC: Backspace, or go back to the status info if password is empty.

3.2 LCD Messages

3.2.1 LCD layout

Line 1	{INFO1}	*
Line 2	{INFO2/DISK}	

Where:

*** :** Heart Plus. The heart plus icon flashes when the controller is working normally. When not flashing, this indicates a controller failure has occurred.

INFO1: Information (including status info, emergent info, and background task messages) display area at line 1, the maximum string length is 15.

INFO2: Information display area at line 2, the maximum string length is 16.

DISK: Disk status display area at line 2. The format is "xxxxxxxxxxxxxxxx".

Each "a" is the HDD status, which are represented as following:

{1, 2, ..., 9, a, b, ... v}: Disk group number, and a means the 10th disk group.

?: Unknown error

A: Adding disk

B: Faulty disk

C: Conflict

F: Foreign disk

G: Global spare disk

I: Initializing

J: JBOD disk

L: Local spare disk

N: Foreign/ Conflict disk

S: Local spare disk

T: Clone-target disk

U: Unused disk

W: SMART warning or BBR alert

X: No disk

INFO2 and **DISK** are mutual exclusive.

3.2.2 Status info

When the system is ready, the system information and background task messages are displayed sequentially every two seconds. See the button functions as below.

UP/DOWN: Scroll up/down the message.

ESC: Clear the message and enter the menu (password may be required).

ENT: Enter the password (if required).

UP+DOWN: Clear all status info and restart to display all the status messages.

Line 1 shows messages, and Line 2 shows the disk status. Messages to be displayed on the LCD panel can be customized by users. The supported status info is listed below:

Status Info	Message	Note
Product name	product name	
Expansion name	Expansion #**x**	#**x**: Expansion ID Up to four expansions can be added.
Date and time	hh:mm MM/DD YY	
IP address	**xxx.xxx.xxx.xxx**	
BP FAN[x] rpm	FAN**x xxxxx**rpm	
Expansion FAN[x] rpm	FAN#**x xxxxx**rpm	
Controller voltage +3.3V	[A] 3.3V: **xx.xx**	3.3V, 5V, and 12V status on controller A or B * [A] denotes controller A; [B] denotes controller B.
Controller voltage +5V	[A] 5.0V: **xx.xx**	
Controller voltage +12V	[A] 12.0: **xx.xx**	
BP voltage +3.3V	[BP] 3.3V: **xx.xx**	3.3V, 5V, and 12V status on backplane
BP voltage +5V	[BP] 5.0V: **xx.xx**	
BP voltage +12V	[BP] 12.0: **xx.xx**	
Expansion voltage sensor[x]	VOLT#**x**: **xx.xx**	
Controller temperature sensor[x]	[A] TEMP**x**: **xx.x**C	Both Celsius (C) and Fahrenheit (F) are supported. Users can customize the temperature scale for the display. * [A] denotes controller A; [B] denotes controller B.
BP temperature sensor[x]	[BP] TEMP**x**: **xx.x**C	
BP average temperature	[BP] AVG: **xx.x**C	
Expansion temperature sensor[x]	TEMP#**x**: **xx.x**C	
Power[x] is %s	Pow**x**: %s	%s: Good, Warning, Error, OFF
Expansion power[x] is %s	Pow#**x**: %s	

Table 3-1 List of status messages

3.2.3 Emergent info

When an emergent event occurs, you can read the message on the LCD. This state is held until every event is confirmed. See the function buttons as below.

UP/DOWN: Scroll up/down the message.

ENT: Confirm (clear) the message. (not supported in current version.)

ESC: Enter the menu (password may be required).

Line 1 shows messages, and Line 2 shows the disk status. The displayed emergent info is listed below:

Emergent Info	Message	Note
Voltage failure	Voltage Failure	
Power failure	Power Failure	
Fan failure	Fan Failure	
Temperature sensor failure	Temp Failure	Temperature warning is not included.
BBM failure	BBM Failure	Only when BBM is present.
Disk SMART warning	SMART Warning	
Disk BBR error	Disk BBR Error	
DG with degraded LD and no rebuild task	DG+Degraded LD	
DG with faulty LD	DG+Faulty LD	
UPS On Batt	UPS On Batt	Only when upsconfig is on.
UPS connection is lost	UPS Con Lost	Only when upsconfig is on.
UPS should be replaced	UPS RB	Only when upsconfig is on.
UPS is overload	UPS Overload	Only when upsconfig is on.
UPS is off	UPS Off	Only when upsconfig is on.

Table 3-2 List of emergent messages

3.2.4 Background task messages

Background tasks and their process percentages are displayed in Line 1. Line 2 shows the disk status. Message formats are listed in the following.

Variables:

xx.yy : xx is the DG identifier; yy is the LD identifier.

dgx : DG identifier.

zz / **HDD z :** HDD identifier.

xx.x% : The progress of task (with percentage estimate)

Background Task	Message Format
LD Expand	**xx.yy** Exp **xx.x**%
LD Migrate	**xx.yy** Mig **xx.x**%
DG Defragment	dg**x** Defrg **xx.x**%
DG Expanding	dg**x** Exp **xx.x**%
Disk Cloning	Clone **zz xx.x**%
Disk Initializing	**xx.yy** Ini **xx.x**%
Disk Rebuilding	Reb **xx xx.x**%
Disk (HDD) Scrubbing	Scrub **zz xx.x**%
LD Scrubbing	**xx.yy** Scr **xx.x**%
DG Scrubbing	dg**x** Scr **xx.x**%
Regenerate LD Parity	**xx.yy** Par **xx.x**%
Regenerate DG Parity	dg**x** Par **xx.x**%

Table 3-3 List of background task messages

3.2.5 Hotkeys

There are four buttons on the LCD console, UP, DOWN, ESC, and ENT. In addition to their basic functions, they can be used in combination for certain hotkey functions.

Hotkey / Key Combinations	Description
UP	View the previous status info message.
DOWN	View the next status info message.
ESC	Enter the menu mode. Skip memory testing when controller boot-up.(Boot-Code v1.03 or latest)
UP+DOWN	Press twice to mute the beeper.
ESC+ENT	Restart to display the local enclosure status info messages.
ENT+UP	Display the previous expansion info message.
ENT+DOWN	Display the next expansion info message.
ESC+UP	(For redundant-controller system only) Press for 2~3 seconds to switch to controller A.
ESC+DOWN	(For redundant-controller system only) Press for 2~3 seconds to switch to controller B.

3.3 Menu

3.3.1 Menu Tree

Use the **UP** or **DOWN** arrow buttons to scroll through the menu. Press the **ENT** button to enter the selected setting. To exit the menu, press **ESC**. The menu tree hierarchy is as shown below:

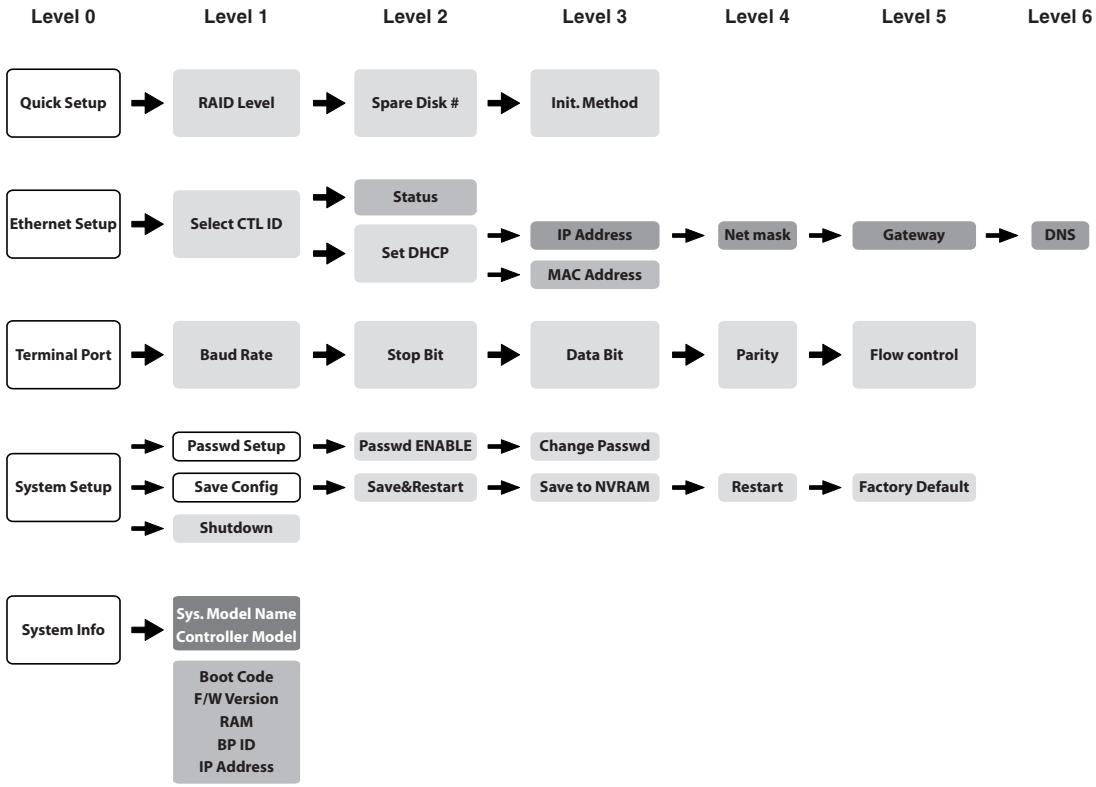


Figure 3-2 Menu tree

3.3.2 Creating an Array

In the **Quick Setup** menu, users can create disk arrays quickly and easily. Configure the following items to create the array. See the options as below.

RAID Level	Level 0 (default), Level 3, Level 5, Level 6, Level 10, Level 30, Level 50, Level 60
Spare Disk #	Default, 1, 2, 3, 4
Init. Method	Background, Foreground (default), No Init

Use the **UP** and **DOWN** buttons to scroll through the options. Press the **ENT** button to select. To cancel the selection and return to the previous level, press the **ESC** button.

3.3.3 Network Settings

In **Ethernet Setup** menu, users can view the network status and configure the server settings. Use the **UP** and **DOWN** buttons to scroll through the following items, and press the **ENT** button to select.

Select CTL ID	(For redundant-controller system only) Selects the controller you want to configure.
Status	Displays the connection status.
Set DHCP	**ENABLE (default) / DISABLE** If DHCP is disabled, the system will require you to enter an IP address, net mask, gateway, and DNS. These settings are configured in the sequence as shown.
MAC Address	Display MAC address.

Users can enter the IP related settings according to the following IP format.

IP format: "xxx.xxx.xxx.xxx", where x is {0, 1, ..., 9}.

Use the **UP** and **DOWN** buttons to select the numbers 0 to 9. Press the **ENT** button to enter the number. To cancel the selection, backspace, and return to the previous level (if IP is empty), press the **ESC** button.

3.3.4 Terminal Port Settings

To configure the settings of terminal port, enter the **Terminal Port** menu. Specify the following items one by one.

Baud Rate	2400, 4800, 9600, 19200, 38400, 57600, 115200 (default)
Stop Bit	1 (default), 2
Data Bit	7, 8 (default)
Parity	NONE (default), ODD, EVEN
Flow control	OFF (default), H/W

Use the **UP** and **DOWN** buttons to scroll through the options. Press the **ENT** button to select it. To cancel the selection and return to the previous level, press the **ESC** button.

3.3.5 System Settings

In the **System Setup** menu, users are allowed to change the password settings, save or restore the configurations to NVRAM, reboot and power off the system. See the following table for details of each option.

Password	**Passwd ENABLE: YES (default) / NO** Enable or disable the password check when logging in menu. **Change Passwd** Key in the new password. The maximum length of password is eight characters. Press and hold the **ESC** button to backspace continuously and return to the previous level.
Save Config	**Save to NVRAM: NO (default) / YES** Save configurations to NVRAM. **Restart: NO (default) / YES** Reboot the system. **Factory: NO (default) / YES** Restore the factory settings to NVRAM.
Shutdown	**NO (default) / YES** Power off the system.

Use the **UP** and **DOWN** buttons to scroll through the items and options. Press the **ENT** button to select. To cancel the selection and return to the previous level, press the **ESC** button.

3.3.6 System Information

The **System Info** menu provides the following information. Use the **UP** and **DOWN** buttons to scroll through each of them. Users are allowed to modify the model name of the system and controller.

Sys. Model Name	Display and modify system model name.
Controller Model*	Display and modify controller model name.
Boot Code*	Display boot code version.
F/W Version*	Display firmware version.
RAM*	Display system memory size.
BP ID*	Display backplane ID number.
IP Address*	Display controller IP address

* Line 1 shows the controller A information, and Line 2 shows the controller B information.

Chapter 4: Using the CLI Commands

4.1 Overview

The Command Line Interface (CLI) is a set of commands which allows users to configure or monitor the RAID system by entering lines of text through a variety of the terminal consoles. Both controller-based embedded CLI and host-side software-based CLI are supported. The Figure 4-1 depicts how the CLI can be accessed:

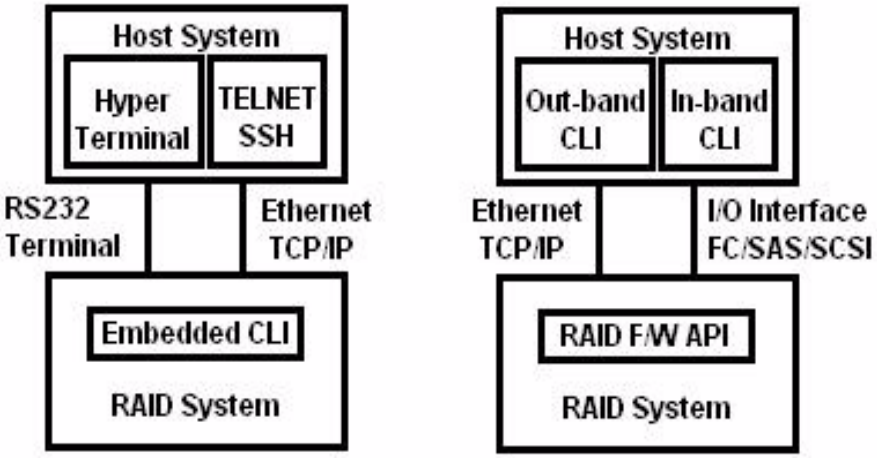


Figure 4-1 Interfaces to Access CLI

With the embedded CLI, you can get full-function management capabilities without the need to install any software on your hosts. But you can access only one system by a terminal at a time.

With the host-side CLI utilities, you may manage multiple RAID systems at one site or apply pre-saved CLI scripts to multiple RAID systems at a time for massive RAID system deployment. The host-side CLI utilities allow you to access RAID systems by in-band (Ethernet) and out-of-band interfaces (FC/ SAS/SCSI).

The login information (login name and password) to the CLI is the same as the login information for Web GUI of the RAID system to be accessed. **0000** is the default login password.

NOTE

The sample code and libraries for developing software to manage RAID systems by in-band or out-band API is available upon request.

4.1.1 Embedded CLI

The embedded CLI can be accessed remotely by the Ethernet (TCP/IP) and locally by the RS232 terminal. And by Ethernet, you may use Telnet and SSH (Secure Shell).

Telnet client software is available for all operating systems, and you can download the SSH client software from the following web sites:

SSHWinClient: **http://www.ssh.com/**

PuTTY: **http://www.chiark.greenend.org.uk/~sgtatham/putty/**

4.1.2 Host-side Out-band CLI Utilities

Out-band CLI communicates with a RAID system by the interface that is different from the I/O interfaces. The RAID system is bundled with the out-band CLI utilities using TCP/IP through the Ethernet port of the RAID controller. You can use CLI on one computer to access RAID systems as long as host computer can reach the RAID systems by the network. The host-side CLI utilities for out-band interface are offered for Windows and Linux.

NOTE

The out-band CLI utility use TCP port 7779 to connect to the RAID system. Please make sure no firewall blocks the traffic on this port.

- **Out-band CLI for Windows**

  To install out-band CLI tool on Windows , copy the **scli-outband-win32-Vx.xx.exe** file to the directory where you want to run the program, and you may start using the CLI utility.

  Installation:

  To install out-band CLI tool on Windows, copy the **scli-outband-win32-Vx.xx.exe** and **isdk-outband-Vx.xx.lib** file to the directory where you want to run the program, and you may start using the CLI utility.

  Usage:

  scli-outband-win32-Vx.xx.exe [-t <controller_ip>][-u <username>] [-p <password>] [-c command]

  Parameters:

  -t <controller_ip>: the IP address of the RAID controller to be accessed

  -u <username>/-p <password>: user name and password

  -c command: the CLI command to be executed

  Example:

  List the status of all hard disks of the RAID system at 168.95.0.1:

  scli-outband-win32-Vx.xx -t 168.95.0.1-u admin -p 0000 -c "hddlist all"

- **Out-band CLI for Linux**

  Installation:

  To install out-band CLI tool on Linux, copy the **cli-outband-linux-Vx.xx** file to the directory where you want to run the program, and you may start using the CLI utility.

  Usage:

  cli-outband-linux-Vx.xx [-t <controller_ip>] [-u <username>] [-p <password>] [-s <script_file>] [-c <command>]

  Parameters:

  -t <controller_ip>: the IP address of the RAID controller to be accessed

  -u <username>/-p <password>: user name and password

  -s <script_file>: the file name that contains CLI scripts to be executed

  -c <command>: the CLI command to be executed

  Examples:

  1. List the status of all hard disks of the RAID system at 168.95.0.1:

     cli-outband-linux-Vx.xx -t 168.95.0.1 -u admin -p 0000 -c "hddlist all"

  2. Enter the interactive mode to access the RAID system at 168.95.0.1:

     cli-outband-linux-Vx.xx -t 168.95.0.1 -u admin -p 0000

  3. Run a CLI script file on the RAID system at 168.95.0.1:

     cli-outband-linux-Vx.xx -t 168.95.0.1 -u admin -p 0000 -s scripet.txt

4.1.3 Host-side In-band CLI Utilities

In-band CLI communicates with a RAID system by the interface that is the same as the I/O interfaces, like FC, SAS, or SCSI, depending on the host interface of your RAID system. Using the in-band CLI frees you from setting up network connections for RAID systems. The host-side CLI utilities for in-band interface are offered for Windows and Linux.

The in-band CLI can work only when there is at least one LUN presented to the host computer running the in-band CLI. When there is no LUN available, a management LUN needs to be set up to transfer the in-band commands. The CLI command, sgmgmtdevice on/off, allows you to enable or disable the management LUN, which is presented to hosts as a SES (SCSI Enclosure Service) device occupying the LUN 127. Contact your HBA vendor if you cannot find the management LUN on your system.

- **In-band CLI for Windows**

Installation:

To install in-band CLI tool on Windows, copy the **scli-inband-win32-Vx.xx.exe** and **isdk-inband-Vx.xx.lib** files to the directory where you want to run the program, and you may start using the CLI utility.

Usage:

scli-inband-win32-Vx.xx [-d <device>] [-u <username>] [-p <password>] -c command

Parameters:

-d <device>: the LUN that the in-band CLI command to be sent

-t <controller_ip>: the IP address of the RAID controller to be accessed

-u <username>/-p <password>: user name and password

-c command: the CLI command to be executed

There are three options to name the LUN on Windows for -d <device>:

1.Drive letter, like "D:"

2.Physical drive number, like "PhysicalDrive2" or "PhysicalDrive5"

3.Adapter, path, target, and LUN, like "scsi2: 0 0 127" or "scsi3: 1 0 127"

If the <device> is not specified, the CLI utility will send the command to the first management LUN detected.

Examples:

1. Scan all HBA and LUNs to discover and display all management LUNs:

   scli-inband-win32-Vx.xx

2. List the status of all hard disks of the RAID system:

   scli-inband-win32-Vx.xx -u admin -p 0000 -c "hddlist all"

NOTE

If a management LUN is presented, you will see a SES device labeled as an unknown device in Windows Device Manager. Windows might prompt you to install the device driver for it. Please ignore it.

- **In-band CLI for Linux**

The in-band command on Linux can be sent only through the SCSI generic (SG) devices (**/dev/sgxx**) to access the management LUN. So, it is required to turn on the management LUN before using in-band CLI

on Linux. You will need also to get root access right to use the in-band CLI. Use the "**modeprobe -v sg**" command to start SCSI generic service if you cannot find any SG devices.

Installation:

To install in-band CLI tool on Linux, copy the cli-inband-linux-Vx.xx file to the directory where you want to run the program, and you may start using the CLI utility.

Usage:

cli-inband-linux-Vx.xx [-d <device>] [-u <username>] [-p <password>] [-s <script_file>] [-c <command>]

Parameters:

-d <device>: the LUN that the in-band CLI command to be sent

-u <username>/-p <password>: user name and password

-s <script_file>: the file name that contains CLI scripts to be executed

-c <command>: the CLI command to be executed

If the <device> is not specified, the CLI utility will send the command to the first management LUN detected in /dev/sgxx.

Examples:

1. Scan all /dev/sgxx to discover and display all management LUNs:
   cli-inband-linux-Vx.xx
2. Enter the interactive mode to for the RAID system at /dev/sg3:
   cli-inband-linux-Vx.xx -d /dev/sg3
3. List the status of all hard disks of the RAID system:
   cli-inband-linux-Vx.xx -u admin -p 0000 -c "hddlist all"
4. Run a CLI script file on the RAID system:
   cli-inband-linux-Vx.xx -u admin -p 0000 -s scripet.txt

NOTE

The following four parameters, <controller_ip>, <device>, <username>, and <password>, are optional. They are not required if you've set the corresponding environment variables before running the CLI utility. Below are the syntax to do so:

set CLI_CTL_IP=<controller_ip>
set CLI_USERNAME=<username>
set CLI_PASSWORD=<password>
set CLI_DEVICE=<device>

NOTE

For both in-band and out-band CLI on Linux, if there is no -c or -s option specified, the CLI utility will automatically enter the interactive mode.

4.1.4 Conventions Overview

Object names

Storage objects are named using the following keywords with an identifier (**x**):

- Hard disk: hdd**x**
- JBOD disk: jbd**x**
- Disk group: dg**x**
- Logical disk: dg**x**ld**y**
- Volume: vol**x**
- Host: host**x**
- Storage group: sg**x**
- Host group: hg**x**
- Logical unit: lun**x**
- Fiber port: fcp**x**
- Serial SCSI port: sas**x**
- Controller: ctl**x**
- Management network port: eth**x**
- Enclosure: enc**x**

Options

Options are expressed in the form of [**-x** ...], where **-x** is the identifier of the option.

Selectable arguments

When more than one value can be used in an argument, they are listed with "/" in between. Users may choose one among them.

Controller modifier

In a dual-controller system, hardware such as the host interface ports is exactly the same on the two controllers. To specify which controller the hardware to be selected in CLI, a controller modifier is added. For example, to refer to the first FC port in controller A, the identifier is °ßfcpa1°®. Without the modifier, all identifiers are referring to local controller (the controller that user logs in currently).

See all the CLI commands and the descriptions in the following sections.

4.2 Basic RAID Management

4.2.1 Hard disks

Command	hddadd
Synopsis	hddadd hdd***x*** hdd***y*** ...
Description	Add hard disks.

Command	hddremove
Synopsis	hddremove hdd***x*** hdd***y*** ...[-p]
Description	Remove hard disks.
Parameters	[-p]: permanent remove

Command	hddlist
Synopsis	hddlist hdd***x***/all [-h]
Description	List the status of one or all hard disks.
Parameters	[-h]: show hardware status

4.2.2 JBOD disks

Command	jbdcreate
Synopsis	jbdcreate jbd***x*** hdd***y*** [-n ***name***] [-c ctl***x***]
Description	Create a JBOD disk by a member disk.
Parameters	[-n ***name***]: the name of a JBOD disk [-c ctl***x***] (for redundant controller only): the preferred controller of a JBOD disk

Command	jbddelete
Synopsis	jbddelete jbd***x*** [-f]
Description	Delete a JBOD disk.
Parameters	[-f]: force to delete LUN mapping

Command	jbdname
Synopsis	jbdname jbd***x name***
Description	Name a JBOD.

Command	jbdlist
Synopsis	jbdlist jbd***x***/all
Description	List the status of one or all JBOD disks.

4.2.3 Disk groups

Command	dgcreate
Synopsis	dgcreate dg***i*** hdd***x*** hdd***y*** ... [-n ***name***] [-i par/seq] [-z] [-s hdd***z***,hdd***a***, ...] [-t ***capacity***]
Description	Create a disk group with member disks.
Parameters	[-n ***name***]: the name of a disk group [-i par/seq]: logical disk initialization mode (parallel or sequential) [-z]: write-zero immediately [-s hdd***z***,hdd***a***, ...]: local spare disks [-t ***capacity***]: capacity to truncate

Command	dgdelete
Synopsis	dgdelete dg***i***
Description	Delete a disk group.

Command	dgname
Synopsis	dgname dg***x name***
Description	Name a disk group.

Command	dginit
Synopsis	dginit dg***i*** par/seq
Description	Set initiation mode of a disk group.

Command	dglist
Synopsis	dglist dg***x***/all
Description	List the status of one or all disk groups.

4.2.4 Spare and rebuild

Command	dgspare
Synopsis	dgspare add/remove dg***i*** hdd***x***
Description	Add or remove a local spare in a disk group.

Command	dgrebseq
Synopsis	dgrebseq dg***i*** par/seq/pri [-l ld***x***,ld***y***, ...]
Description	Set rebuild mode of a disk group.
Parameters	par/seq/pri: parallel, sequential, or priority [-l ld***x***,ld***y***, ...]: priority of logical disks to rebuild

Command	globalspare
Synopsis	globalspare add/remove hdd***x*** hdd***y*** ...
Description	Add or remove one or more hard disks as global spare disks.

Command	autospare
Synopsis	autospare [on/off]
Description	Review or set the auto spare settings.
Parameters	[on/off]: turn on or off the auto spare option

Command	restorespare
Synopsis	restorespare [on/off]
Description	Review or set the restore spare settings.
Parameters	[on/off]: turn on or off the restore spare option

4.2.5 Logical disks

Command	ldcreate
Synopsis	ldcreate dg**x**ld**y** ***capacity raidlevel*** [-s ***stripesize***] [-i ***initopt***] [-f **x**] [-o ***offset***] [-n ***name***] [-c ctl**x**]
Description	Create a logical disk.
Parameters	***capacity***: logical disk capacity ***raidlevel***: raid0, raid5, raid3, raid1, raid6, raid10, or nraid [-s ***stripesize***]: stripe size [-i ***initopt***]: initialization method [-f **x**]: free chunk [-o ***sector***]: alignment offset [-n ***name***]: the name of a logical disk [-c ctl**x**] (for redundant controller only): the preferred controller of a logical disk

Command	lddelete
Synopsis	lddelete dg**x**ld**y** [-f]
Description	Delete a logical disk.
Parameters	[-f]: force to delete LUN mapping

Command	ldname
Synopsis	ldname dg**x**ld**y** ***name***
Description	Name a logical disk.

Command	ldlist
Synopsis	ldlist dg**x**ld**y**/dg**x**/all
Description	List the status of one logical disk, all logical disks on a disk group, or al logical disks on the controller.

4.2.6 RAID algorithms options

Command	intellicompute
Synopsis	intelicompute dg**x**ld**y**/all on/off
Description	Enable or disable Intelligent data computation for one or all RAID 3/5/6 logical disks.

Command	readmaxtime
Synopsis	readmaxtime dg**x**ld**y**/all **xx**msec
Description	Specify the maximum response time for one or all RAID 3/5/6 logical disks.

Command	checkonread
Synopsis	checkonread dg***x***ld***y***/all on/off
Description	Enable or disable check-on-read for all RAID 3/5/6 logical disks.

Command	writelog
Synopsis	writelog [on/off]
Description	Review or set the write logging.
Parameters	[on/off]: enable or disable write logging

4.2.7 Volumes

Command	volcreate
Synopsis	volcreate vol***x*** dg***x***ld***y*** dg***i***ld***j*** ...[-s ***stripesize***] [-o ***sector***] [-n ***name***] [-c ctl***x***]
Description	Create a volume.
Parameters	[-s ***stripesize***]: stripe size [-o ***sector***]: alignment offset [-n ***name***]: the name of a volume [-c ctl***x***] (for redundant controller only): the preferred controller of a volume

Command	voldelete
Synopsis	voldelete vol***x*** [-f]
Description	Delete a volume.
Parameters	[-f]: force to delete LUN mapping

Command	volname
Synopsis	volname vol***x*** ***name***
Description	Name a volume.

Command	vollist
Synopsis	vollist vol***x***/all
Description	List the status of one or all volumes.

4.2.8 Cache

Command	readahead
Synopsis	readahead vol***x***/dg***x***ld***y***/jbd***x***/all ***policy*** [-m ***multiplier***] [-l ***read_log***]
Description	Enable or disable read ahead policy of a volume, a logical disk, a JBOD disk, or all virtual disks.
Parameters	***policy***: always, adaptive, or off [-m ***multiplier***]: set read-ahead multiplier [-l ***read_log***]: set number of read logs

Command	writecache
Synopsis	writecache vol***x***/dg***x***ld***y***/jbd***x***/all on/off [-s on/off]
Description	Enable or disable write cache of a volume, a logical disk, a JBOD disk, or all buffers.
Parameters	[-s on/off]: enable or disable the write sorting

Command	cachepflush
Synopsis	cachepflush [***period***sec]
Description	Review or set the current cache flush period.
Parameters	[***period***sec]: the cache flush period

Command	cacheunit
Synopsis	cacheunit [4kb/8kb/16kb/32kb/64kb/128kb]
Description	Review or set the cache unit size.
Parameters	[4kb/8kb/16kb/32kb/64kb/128kb]: set cache unit size

Command	cacheflush
Synopsis	cacheflush vol***x***/dg***x***ld***y***/jbd***x***/all [-w ***xx***min]
Description	Flush write buffers in the write cache of a volume, a logical disk, a JBOD disk, or all write buffers in the cache.
Parameters	[-w ***xx***min]: number of minutes to wait for flush completion

Command	cachedirtyratio
Synopsis	cachedirtyratio [***dirty_ratio***]
Description	Review or set the dirty buffer ratio.
Parameters	[***dirty_ratio***]: dirty buffer ratio

Command	cachelist
Synopsis	cachelist vol***x***/dg***x***ld***y***/jbd***x***/all
Description	List the setting and status of a volume, a logical disk, a JBOD disk.

4.3 RAID Maintenance Utilities

4.3.1 RAID attributes reconfiguration utilities

Command	dgexpand
Synopsis	dgexpand dg***i*** [-d] hdd***x*** hdd***y*** ...
Description	Expand a disk group by adding one or more disks.
Parameters	[-d]: defragment during expanding

Command	ldmigrate
Synopsis	ldmigrate dg***x***ld***y*** [-s ***newstripesize***] [-r ***newraidlevel***] [-d] [-l hdd***x***,hdd***y***,...]
Description	Perform RAID level and/or stripe size migration for a logical disk on a disk group. At least one option must be set.
Parameters	[-s ***newstripesize***]: migrate to new stripe size [-r ***newraidlevel***]: migrate to new RAID level [-d]: defragment during migration [-l hdd***x***,hdd***y***,...]: expanding disk group by adding these hard disks

Command	ldexpand
Synopsis	ldexpand dg***i***ld***x*** ***newcapacity*** [-i ***initopt***] [-f ***x***,***y***]
Description	Expand the capacity of one or more logical disks in a disk group.
Parameters	***newcapacity***: new capacity of a logical disk [-i ***initopt***]: initialization method [-f ***x***,***y***]: free chunks

Command	ldshrink
Synopsis	ldshrink dg***i***ld***x*** ***newcapacity***
Description	Shrink the capacity of a logical disk.
Parameters	***newcapacity***: new capacity of a logical disk

Command	dgdefrag
Synopsis	dgdefrag dg***i***
Description	Defragment a disk group.

Command	volexpand
Synopsis	volexpand vol**x** dg***i***ld**x** dg***j***ld***y***
Description	Expand a volume by concatenating new logical disks.

Command	volshrink
Synopsis	volshrink vol**x**
Description	Shrink the capacity of a volume by removing the concatenating logical disks.

4.3.2 Data integrity maintenance utilities

Command	hddclone
Synopsis	hddclone hdd**x** hdd***y*** [-a]
Description	Perform disk cloning (clone from hdd**x** to hdd***y***).
Parameters	[-a]: automatic resume

Command	hddclonestop
Synopsis	hddclonestop hdd**x**
Description	Stop disk cloning.

Command	diskscrub
Synopsis	diskscrub dg**x**/dg**x**ld***y***/hdd**x** [-c] [-g]
Description	Perform disk scrubbing in a disk group, a logical disk, or a hard disk.
Parameters	[-c]: parity check [-g]: regenerate

Command	diskscrubstop
Synopsis	diskscrubstop dg**x**/dg**x**ld***y***/hdd**x**
Description	Stop disk scrubbing in a disk group, a logical disk, or a hard disk.

Command	regparity
Synopsis	regparity dg**x**/dg**x**ld***y***
Description	Regenerate the parity of a logical disk or the logical disks of disk group with parity-based RAID level.

Command	regparitystop
Synopsis	regparitystop dg***x***ld***y***/dg***x***
Description	Stop regenerating parity of a logical disk or the logical disks of disk group with parity-based RAID level.

4.3.3 Task priority control

Command	hddutilpri
Synopsis	hddutilpri [***priority***]
Description	Show or set the utilities task priority of non-DG hard disks.
Parameters	[***priority***]: low, medium, or high

Command	dgrebpri
Synopsis	dgrebpri dg***x priority***
Description	Set the rebuild task priority of a disk group.
Parameters	***priority***: low, medium, or high

Command	dginitpri
Synopsis	dginitpri dg***x priority***
Description	Set the initialization task priority of a disk group.
Parameters	***priority***: low, medium, or high

Command	dgutilpri
Synopsis	dgutilpri dg***x priority***
Description	Set the utilities task priority of a disk group.
Parameters	***priority***: low, medium, or high

4.3.4 Task schedule management

Command	schedulecreate
Synopsis	schedulecreate [-s ***YYYY/MM/DD/hh/mm***]/[-m ***DD/hh/mm***]/ [-w ***WD/hh/mm***] ***command***
Description	Create a schedule or a periodic schedule for a CLI command.
Parameters	[-s ***YYYY/MM/DD/hh/mm***]: the target date/time [-m ***DD/hh/mm***]: monthly [-w ***WD/hh/mm***]: weekly ***command***: commands allowed to be scheduled include ***dgexpand***, ***dgdefrag***, ***ldmigrate***, ***ldexpand***, ***hddclone***, ***diskcrub***, ***regparity*** and ***hdddst***

Command	scheduledelete
Synopsis	scheduledelete ***schedule_id***
Description	Delete a schedule with the schedule ID.

Command	schedulelist
Synopsis	schedulelist ***command***/all
Description	List one or all types of scheduled commands.

4.3.5 On-going task monitoring

Command	tasklist
Synopsis	tasklist ***command***/all
Description	List one or all types of background tasks.

Command	tasknotify
Synopsis	tasknotify on/off [-p ***percentage***]
Description	Enable or disable the event notification of the background task completion.
Parameters	[-p ***percentage***]: completion percentage to notify

4.3.6 Array and volume roaming

Command	autoroam
Synopsis	autoroam on/off
Description	Enable or disable automatic array roaming when the controller is started.

Command	onlineroam
Synopsis	onlineroam on/off
Description	Enable or disable on-line array roaming.

Command	hddimport
Synopsis	hddimport [-f][-t jbd***x***/dg***x***] all/hdd***x*** hdd***y*** hdd***z*** ...
Description	Import all or specified foreign/conflict hard disks.
Parameters	[-f]: force to import an incomplete disk group with degraded logical disks [-t jbd***x***/dg***x***]: target disk to restore

Command	hddimportlist
Synopsis	hddimportlist all/hdd***x*** hdd***y*** hdd***z*** ...
Description	List all or specified foreign/conflict hard disks with the configurations stored on the hard disks.

Command	volimport
Synopsis	volimport [-f][-t vol***x***] dg***x***ld***y*** dg***i***ld***j*** ...
Description	import a volume from logical disks specified.
Parameters	[-f]: force to import a faulty volume [-t vol***x***]: target volume

Command	volimportlist
Synopsis	volimportlist all/dg***x*** dg***y*** ...
Description	List volume configurations on all or specified logical disks.

4.3.7 Array recovery utilities

Command	dgrecover
Synopsis	dgrecover dg***x*** hdd***x*** hdd***y*** ... [-f ***member_id***]
Description	Recover a faulty disk group.
Parameters	[-f ***member_id***]: force to recover disk

Command	ldrecover
Synopsis	ldrecover dg***x***ld***y*** ***partition_id***
Description	Recover a faulty logical disk.

Command	volrecover
Synopsis	volrecover vol***x*** dg***i***ld***j*** dg***x***ld***y*** ...
Description	Recover a faulty volume.

4.4 Storage Presentation

4.4.1 Hosts

Command	hostcreate
Synopsis	hostcreate host***x*** ***WWN*** [-n ***name***]
Description	Create a host with WWN.
Parameters	[-n ***name***]: host name

Command	hostdelete
Synopsis	hostdelete host**x** host**y** ...
Description	Delete hosts.

Command	hostname
Synopsis	hostname host**x** ***name***
Description	Name a host.

Command	hostlist
Synopsis	hostlist all/host**x**
Description	List all hosts or one host.

4.4.2 Host groups

Command	hgaddhost
Synopsis	hgaddhost hg**x** host**x** host**y** ...
Description	Add hosts to a host group.

Command	hgremovehost
Synopsis	hgremovehost hg**x** host**x** host**y** ...
Description	Remove hosts from a host group.

Command	hgname
Synopsis	hgname hg**x** ***name***
Description	Name a host group.

Command	hglist
Synopsis	hglist hg**x**/all
Description	List one or all host groups.

4.4.3 Storage groups

Command	sgaddlun
Synopsis	sgaddlun sg**x**/fcp**x**/sas**x**/scp**x** jbd**y**/dg**y**ld**z**/vol**y**/vvol**y** [-l lun**z**] [-s 512b/1kb/2kb/4kb] [-g ***cylinder head sector***] [-w wt/wb]
Description	Add a LUN in a storage group or a default storage group.
Parameters	[-l lun**z**]: LUN to be used by the virtual disk [-s 512b/1kb/2kb/4kb]: set sector size [-g ***cylinder head sector***]: set the cylinder/head/sector mapping of the LUN [-w wt/wb]: write completion (write-through or write-behind)

Command	sgremovelun
Synopsis	sgremovelun sg**x**/fcp**x**/sas**x**/scp**x** lun**y**/all
Description	Remove one or all LUNs in a storage group or a default storage group.

Command	sgremovedisk
Synopsis	sgremovedisk sg**x**/fcp**x**/sas**x**/scp**x**/all jbd**y**/dg**y**ld**z**/vol**y**/ vvol**y**
Description	Remove LUNs of a virtual disk from one storage groups, a default storage group, or all storage groups.

Command	sgmasklun
Synopsis	sgmasklun sg**x**/fcp**x**/sas**x** lun**y**/all
Description	Mask one or all LUNs in a storage group or a default storage group.

Command	sgunmasklun
Synopsis	sgunmasklun sg**x**/fcp**x**/sas**x** lun**y**/all
Description	Unmask one or all LUNs in a storage group or a default storage group.

Command	sgaccess
Synopsis	sgaccess sg**x**/fcp**x**/sas**x**/scp**x** all/lun**y** ro/rw
Description	Set LUN access right of one or all LUNs in a storage group or a default storage group.
Parameters	ro/rw: read-only or read-writable

Command	sgname
Synopsis	sgname sg***x name***
Description	Name a storage group.

Command	sglistlun
Synopsis	sglistlun sg**x**lun**y**/fcp**x**lun**y**/sas**x**lun**y**/scp**x**lun**y**/sg**x**/fcp**x**/sas**x**/ scp**x**/all
Description	List LUN information in one or all storage groups / default storage groups.

4.4.4 Presentation planning

Command	sgsetmethod
Synopsis	sgsetmethod ***sim/sym/sel***
Description	Select storage presentation method.
Parameters	***sim/sym/sel***: simple, symmetric-LUN, or selective storage presentation [-a on/off]: enable or disable automatic LUN mapping

Command	sgmgmtdevice
Synopsis	sgmgmtdevice on/off [*-l lun***x**]
Description	Enable or disable management device support of in-band API.
Parameters	[*-l lun***x**]: This option specifies the LUN be used by the management device. default is LUN 127. ***Note:****SCSI host interface system, the default is LUN 15*

4.4.5 Selective storage presentation

Command	htpbind
Synopsis	htpbind fcp**x**/sas**x**/all sg**y** host**z**/hg**z**
Description	Bind a storage group to one or all FC ports for a host or a host group.

Command	htpunbind
Synopsis	htpunbind fcp**x**/sas**x**/all host**z**/hg**z**
Description	Unbind a host or a host group from one or all FC ports.

Command	htplist
Synopsis	htplist fcp**x**/sas**x**/all
Description	List all storage groups bound to one or all FC ports.

4.4.6 Simple storage presentation

Command	htpaddlun
Synopsis	htpaddlun fcp***x***/sas***x*** jbd***y***/dg***y***ld***z***/vol***y***/vvol***y*** [-l lun***z***] [-s 512b/1kb/2kb/4kb] [-g ***cylinder head sector***] [-w wt/wb] htpaddlun scp***x*** jbd***y***/dg***y***ld***z***/vol***y***/vvol***y*** [-i ***scsi_id***] [-l lun***z***] [-s 512b/1kb/2kb/4kb] [-g ***cylinder head sector***] [-w wt/wb]
Description	Add a LUN in a FC port with a virtual disk.
Parameters	[-i ***scsi_id***]: SCSI ID Refer to **sgaddlun** for other parameters.

Command	htpremovelun
Synopsis	htpremovelun fcp***x***/sas***x*** lun***y***/all htpremovelun scp***x*** id***x***/id***x***lun***y***/all
Description	Remove one or all LUNs in a host port.

Command	htpremovedisk
Synopsis	htpremovedisk fcp***x***/sas***x***/scp***x***/all jbd***y***/dg***y***ld***z***/vol***y***/vvol***y***
Description	Remove all LUNs of a virtual disk from one or all host ports.

Command	htplistlun
Synopsis	htplistlun fcp***x***/sas***x***/scp***x***/all
Description	List LUN information in one or all host ports.

4.4.7 Symmetric-LUN storage presentation

Command	hgaddlun
Synopsis	hgaddlun hg***x*** jbd***y***/dg***y***ld***z***/vol***y***/vvol***y*** [-l lun***z***] [-s 512b/1kb/2kb/4kb] [-g ***cylinder head sector***] [-w wt/wb]
Description	Add a LUN in a host group with a virtual disk.
Parameters	Refer to **sgaddlun** for all parameters.

Command	hgremovelun
Synopsis	hgremovelun hg***x*** lun***y***/all
Description	Remove one or all LUNs from a host group.

Command	hgremovedisk
Synopsis	hgremovedisk hg***x***/all jbd***y***/dg***y***ld***z***/vol***y***/vvol***y***
Description	Remove all LUNs of a virtual disk from one or all host groups.

Command	hglistlun
Synopsis	hglistlun hg**x**/all
Description	List LUN information in one or all host groups.

4.5 Hardware Configurations and Utilities

4.5.1 Generic hard disk

Command	hddst
Synopsis	hdddst short/extended all/hdd**x** hdd**y** hdd**z** …
Description	Perform short or extended disk self test (DST).

Command	hdddststop
Synopsis	hdddststop all/hdd**x** hdd**y** hdd**z** …
Description	Stop DST immediately.

Command	hdddstlist
Synopsis	hdddstlist all/hdd**x** hdd**y** hdd**z** …
Description	List disk self test information and status.

Command	hddsmart
Synopsis	hddsmart on [-p ***period***] [-a clone/alert] hddsmart off
Description	Change the SMART warning settings of all hard disks.
Parameters	on/off: SMART control [-p ***period***]: period of SMART polling [-a clone/alert]: SMART actions

Command	hddsmartlist
Synopsis	hddsmartlist all/hdd**x** hdd**y** hdd**z** …
Description	List SMART information and current status of the specified or all hard disks.

Command	hddsmartread
Synopsis	hddsmartread hdd**x**
Description	Display the SMART data of a hard disk.

Command	hddbbralert
Synopsis	hddbbralert on/off [-p ***percentage1 percentage2 percentage3 percentage4***]
Description	Enable or disable event alerts for bad block reallocation.
Parameters	[-p ***percentage1 percentage2 percentage3 percentage4***]: thresholds to alert

Command	hddbbrclone
Synopsis	hddbbrclone on/off [-p ***percentage***]
Description	Enable or disable disk cloning for bad block reallocation.
Parameters	[-p ***percentage***]: thresholds to start cloning

Command	hddbbrretry
Synopsis	hddbbrretry on/off
Description	Enable or disable retrying IO in bad block reallocation.

Command	hddcache
Synopsis	hddcache on/off all/dg**x**/hdd**x**
Description	Enable or disable the disk cache of a hard disk, hard disks in a disk group, or all hard disks.

Command	hddstandby
Synopsis	hddstandby on/off
Description	Enable or disable the hard disk standby state.

Command	hddidentify
Synopsis	hddidentify on/off hdd**x**/dg**x**
Description	Enable or disable visual identification of a hard disk or disk group.

Command	hddtimeout
Synopsis	hddtimeout **xx**sec
Description	Specify the timeout value of a IO command sent to hard disks.

Command	hddretry
Synopsis	hddretry **xx**
Description	Specify the number of retries when a disk IO command fails.

Command	hddxfermode
Synopsis	hddxfermode ***mode***
Description	Specify the transfer mode of hard disks in the enclosure. The possible values of mode are Auto(default), 1.5Gb,and 3Gb.

Command	hddqueue
Synopsis	hddqueue on/off
Description	Enable or disable the IO queuing of hard disks.

Command	hdddelayaccess
Synopsis	hdddelayaccess [-b] ***xx***sec
Description	Specify the delay time before the controller tries to access the hard disks after power-on.
Parameters	[-b]: boot-up delay access time

Command	hddverify
Synopsis	hddverify on/off
Description	Enable or disable the write commands for initialization or rebuilding data on logical disks.

Command	hddlistconf
Synopsis	hddlistconf
Description	List the current hardware configurations of all hard disks.

4.5.2 SAS ports

Command	sasname
Synopsis	sasname sas**x** name
Description	You can sets the name of a SAS port, sasx, as name. The default is "sas**x**".

Command	saslistcurconf
Synopsis	saslistcurconf sas**x**/all
Description	Displays the current configurations of a SAS port (sas**x**) or all SAS ports (all).

4.5.3 SCSI ports

Command	scpname
Synopsis	scpname scp**x** name

Description	You can sets the name of a SCSI port, scpx, as name. The default is "scp**x**".

Command	scprate
Synopsis	scprate scp**x**/all async/fast/fastwide/ultra/ultrawide/ultra2/ ultra2wide/ultra3/ultra320
Description	You can sets the preferred data rate of a SCSI port (scp**x**) or all SCSI ports (all), as Asynchrous SCSI (async), Fast SCSI (fast), Fast-Wide SCSI (fastwide), Ultra SCSI(ultra), Ultra Wide SCSI (ultrawide), Ultra2 SCSI (ultra2), Ultra2 Wide SCSI(ultra2wide), Ultra3 SCSI (ultra3), or Ultra-320 SCSI (ultra320),The default is ultra320.

Command	scpdefid
Synopsis	scpdefid scp**x** scsi_id
Description	you can sets the default SCSI ID of a SCSI port (scp**x**) to scsi_id which valid value are 0~15. The default SCSI ID is 0.

Command	scplistusrconf
Synopsis	scplistusrconf scp**x**/all
Description	Displays the user configurations of a SCSI port (scp**x**) or all SCSI ports (all).

Command	scplistcurconf
Synopsis	scplistcurconf scp**x**/all
Description	Displays the current configurations of a SCSI port (scp**x**) or all SCSI ports (all).

4.5.4 FC ports

Command	fcpname
Synopsis	fcpname fcp***x name***
Description	Name an FC port.

Command	fcploopid
Synopsis	fcploopid fcp***x id***/auto
Description	Set the hard loop ID of an FC port.
Parameters	***id***: hard loop ID auto: automatically determined

Command	fcpconmode
Synopsis	fcpconmode fcp**x**/all al/fabric/auto
Description	Set the connection mode of an FC port or all FC ports.
Parameters	al/fabric/auto: arbitration loop, fabric, or automatically determined

Command	fcprate
Synopsis	fcprate fcp**x**/all 1gb/2gb/4gb/auto
Description	Set the prefered data rate of an FC port or all FC ports.
Command	fcpwwnn
Synopsis	fcpwwnn identical/distinct
Description	Set the World-Wide Node Name of FC port to be identical or distinct. Without option, this command shows the current setting.

Command	fcplisthost
Synopsis	fcplisthost fcp**x**/all
Description	List the detected hosts of an FC port or all FC ports.

Command	fcplistusrconf
Synopsis	fcplistusrconf fcp**x**/all
Description	List the user's configurations of an FC port or all FC ports.

Command	fcplistusrconf
Synopsis	fcplistcurconf fcp**x**/all
Description	List the current configurations of an FC port or all FC ports.

4.5.5 Management network interface

Command	ethsetaddr
Synopsis	ethsetaddr eth***x method*** [-a] ***ip_addr*** [-s] ***net_mask*** [-g] ***gw_addr*** [-d] ***dns_addr*** [-z] ***on/off***
Description	Set IP address of an Ethernet port.
Parameters	***method***: static or dhcp [-a]: network address [-s]: network mask [-g]: gateway address [-d]: DNS server address [-z]:Automatic Private IP Addressing (APIPA)

Command	ethlistaddr
Synopsis	ethlistaddr eth***x***
Description	List IP and MAC address of an Ethernet port.

Command	smtpconfig
Synopsis	smtpconfig set primary/secondary ***server sender*** [-p ***password***] [-n ***name***] smtpconfig reset primary/secondary
Description	Configure or clear the primary or secondary SMTP servers.
Parameters	set/reset: set or reset SMTP server ***server***: the SMTP server address ***sender***: the account on SMTP server [-p ***password***]: the password of the account on SMTP server [-n ***name***]: name to be shown on the sender field

Command	smtplist
Synopsis	smtplist
Description	List the SMTP configurations.

Command	smtptest
Synopsis	smtptest primary/secondary ***receiver***
Description	Send a test mail via primary or secondary mail server to a mail account.
Parameters	***receiver***: mail address of receiver

Command	ethlist
Synopsis	ethlist
Description	Show the control settings of all management network interface ports.

4.5.6 Local terminal ports

Command	termconf
Synopsis	termconf [***baud_rate stop_bit data_bit parity flow_ctrl***]
Description	Review or set the terminal.
Parameters	***baud_rate***: 2400, 4800, 9600, 19200, 38400, 57600, or 115200) ***stop_bit***: 1 or 2 ***data_bit***: 7 or 8 ***parity***: parity check (none, even, or odd) ***flow_ctrl***: flow control (none or hw)

4.5.7 Enclosure

Command	encpoll
Synopsis	encpoll **xx**sec
Description	Specify the polling interval, at which the controller polls the enclosure controller in the external enclosure to acquire the status of the enclosure.

Command	enclist
Synopsis	enclist enc***x element***/all
Description	List the current status of one or all management elements of an enclosure.
Parameters	***element*** could be one of the following values: spow/vlt/crt/ fan/tm. Each of which means power supply, voltage sensor, current sensor, fan, and temperature sensor.

Command	enclist conf
Synopsis	enclistconf
Description	List enclosure configurations.

Command	encidentify
Synopsis	encidentify on/off enc***x***
Description	Enable or disable identifying the enclosure with a visual indication. This command is applicable only when enclosure visual indication hardware is available.

Command	encfwupdate
Synopsis	enfwupdate enc***x firmware.bin***
Description	Update the firmware of the controller in an external enclosure with the specified firmware file.

4.5.8 Uninterruptible power supply

Command	upscontrol
Synopsis	upscontrol on/off
Description	Enable or disable UPS support.

Command	upslist
Synopsis	upslist
Description	List UPS information.

Command	upsconfig

Synopsis	upsconfig [-d ***YY/MM/DD***] [-l **xx**sec] [-r **xx**%] [-s **xx**sec] [-b **xx**sec]
Description	Set UPS configurations. At least one option should be assigned.
Parameters	[-d ***YYYY/MM/DD***]: date of last battery replacement [-l **xx**sec]: low battery runtime threshold [-r **xx**%]: minimum battery charge capacity before restart [-s **xx**sec]: UPS delay power off in seconds [-b **xx**sec]: UPS delay power on in seconds

4.6 Performance management

4.6.1 Hard disks

Command	hddstat
Synopsis	hddstat on/off/reset
Description	Change the setting of hard disk IO logging.

Command	hddliststat
Synopsis	hddliststat hdd**x**
Description	List hard disk IO statistics.

4.6.2 Cache

Command	cachestat
Synopsis	cachestat on/off/reset
Description	Change the setting of cache IO logging.

Command	cachestatlist
Synopsis	cachestatlist vol**x**/dg**x**ld**y**/jbd**x**/all
Description	List cache IO statistics.

4.6.3 LUN

Command	lunstat
Synopsis	lunstat on/off/reset
Description	Change the setting of LUN IO logging.

Command	lunliststat
Synopsis	lunliststat sg**x**lun**y**/fcp**x**lun**y**/sas**x**lun**y**/scp**x**id**y**lun**z**/hg**x**lun**y**
Description	List LUN IO statistics.

4.6.4 Storage ports

Command	fcpstat
Synopsis	fcpstat on/off/reset
Description	Enable or clear FC port statistics.

Command	fcpliststat
Synopsis	fcpliststat fcp**x**
Description	List FC port IO statistics.

Command	sasstat
Synopsis	sasstat on/off/reset
Description	Enable or clear SAS port statistics.

Command	saslistat
Synopsis	saslistat fcp**x**
Description	List SAS port IO statistics.

4.7 Redundant Controller Configurations

4.7.1 Mirrored write cache control

Command	cachemirror
Synopsis	cachemirror [on/off]
Description	Show or change the setting of mirrored write cache control.
Parameters	[on/off]: enable or disable mirrored write cache

4.7.2 Change preferred controller

Command	prefctlchg
Synopsis	prefeclchg [-o] jbd**x**/dg**x**ld**y**/vol**x** ctl**x**
Description	Change the preferred controller of a virtual disk.
Parameters	[-o]: change owner controller immediately

4.7.3 Path failover alert delay

Command	foalertdelay
Synopsis	foalertdelay [**xx**min]
Description	Set the delay period before the controller generates a warning event to notify users of the critical condition that virtual disks transferred to the non-preferred controller.

4.8 Event Management

4.8.1 NVRAM event logs

Command	eventlist
Synopsis	eventlist [-f **xx**] [-n **xx**] [-s ***severity***]
Description	List records in the event log from older to newer records.
Parameters	[-f **xx**]: starting point of event to list [-n **xx**]: maximum number of records to list [-s ***severity***]: severity level of records to list

Command	eventget
Synopsis	eventget log.txt/log.csv
Description	Download all event records to a file, log.txt or log.csv.

Command	eventconfig
Synopsis	enentconfig [-s ***severity***]
Description	List or configure the lowest severity level of events to be recorded.
Parameters	[-s ***severity***]: severity level of events to record

Command	eventerase
Synopsis	eventerase
Description	Erase all records in the event log.

Command	eventtest
Synopsis	enenttest ***severity***
Description	Generate a testing event record with the specified severity level.

4.8.2 Event notification

Command	notifycontrol
Synopsis	notifycontrol on/off smtp/snmp/all
Description	Enable or disable event notifications of all or the selected notification method.

Command	notifylist
Synopsis	notifylist smtp/snmp/all
Description	List the current settings of all or the selected notification method.

Command	eventmailrcv
Synopsis	eventmailrcv set rcv***x receiver severity*** eventmailrcv reset rcv***x***
Description	Enable or disable the specified mail account for mail notification receiver.
Parameters	set/reset: set or clear receiver rcv***x***: receiver identifier ***receiver***: mail address of receiver ***severity***: severity level to notify

Command	eventmailconfig
Synopsis	eventmailconfig [-j ***subject***] [-r ***x***min] [-d ***x***sec] [-c ***content***]
Description	Display or set the event mail configurations.
Parameters	[-j ***subject***]: event mail subject [-r ***x***min]: event mail retry period [-d ***x***sec]: event mail delay time [-c ***content***]: event mail content

Command	snmptraprcv
Synopsis	snmptraprcv set rcv***x server port version community severity*** snmptraprcv reset rcv***x***
Description	Enable or disable the specified SNMP server for SNMP trap notification receiver.
Parameters	set/reset: set or clear receiver rcv***x***: receiver identifier ***server***: SNMP server address ***port***: SNMP server port number ***version***: SNMP protocol version ***community***: SNMP community name ***severity***: severity level to notify

Command	snmptraptest
Synopsis	snmptraptest rcv***x***
Description	Send a test SNMP trap to the specified server.

Command	snmpagent
Synopsis	snmpagent on [*-p* ***port***] [-c ***community***]
Description	Enable or disable the SNMP agent which allow SNMP browser to obtain information from the controller.
Parameters	[*-p* ***port***]: SNMP agent port number [-c ***community***]: SNMP community name

4.8.3 Event handling

Command	autowritethrough
Synopsis	autowritethrough [on/off ctl/bbm/pow/fan/ups]
Description	Review or set the auto write-through function.
Parameters	ctl/bbm/pow/fan/ups: controller failure, battery backup module failure, power supply unit failure, fan failure, or UPS failure

Command	autoshutdown
Synopsis	autoshutdown [on/off] [-e upsac/fan/temp] [-t ***xx***min]
Description	Review or set the auto shutdown function.
Parameters	[on/off]: enable or disable the auto shoutdown function [-e upsac/fan/temp]: event to trigger auto shutdown. (UPS AC power loss and then low battery or UPS connection loss, all fan failure, or over temperature) [-t ***xx***min]: shutdown delay time

4.9 System Management

4.9.1 Configurations management

Command	configrestore
Synopsis	configrestore [-h]
Description	Erase all configurations on NVRAM or hard disks and restore to factory default.
Parameters	[-h]: erase configurations on all hard disks instead of NVRAM

Command	configerase
Synopsis	configerase hdd***x*** hdd***y*** …
Description	Erase controller's configurations stored on hard disks.

Command	configtohdd
Synopsis	configtohdd hdd***x***
Description	Save NVRAM configurations to a hard disk.

Command	configfromhdd
Synopsis	configfromhdd hdd***x***
Description	Restore NVRAM configurations from hard disks.

Command	configget
Synopsis	configget ***config.bin***
Description	Get main configurations stored on NVRAM and save to a file, config.bin.

Command	configset
Synopsis	configset ***config.bin***
Description	Store a file, config.bin, as the controller's main configurations on NVRAM.

Command	configtext
Synopsis	configtext ***config.html***
Description	Get the main configurations and save to a html file.

Command	configtextmail
Synopsis	configtextmail ***account***
Description	Get the main configurations and save to a text file, which is then sent to the specified mail receiver.

Command	confighdd
Synopsis	confighdd [***frequency***]
Description	Show or update the progress of background tasks except reconfiguration task.
Parameters	[***frequency***]: high, medium, or low

4.9.2 Time management

Command	dateset
Synopsis	dateset static/ntp [-t ***YYYY/MM/DD/hh/mm***]/[-n ***xxx.yyy.zzz***]
Description	Set the current date and time on the controller.
Parameters	[-t ***YYYY/MM/DD/hh/mm***]: date and time. This is valid only when static is specified. [-n ***xxx.yyy.zzz***]: NTP server network address. This is valid only when ntp is specified.

Command	timezoneset
Synopsis	timezoneset -**z Area/Location** [-*d* ***on/off***] timezoneset -**i**
Description	Set the time zone.
Parameters	[-**i**]: Interactive mode [-**z Area/Location**]: Time zone name of area and location [-*d* ***on/off***]: Daylight saving time (DST) setting

Command	ntpsync
Synopsis	ntpsync
Description	Immediately synchronize controller's time with network time server.

Command	datelist
Synopsis	datelist

Description	List the current date, time, and time zone on the controller.

4.9.3 Administration security control

Command	login
Synopsis	login ***username*** [-t ***target_controller***]
Description	Login into CLI with an account and its password.
Parameters	***username***: enter the user name [-t ***target_controller***]: enter the IP address of the RAID subsystem the users want CLI to log in

Command	passwd
Synopsis	passwd user/admin ***old_password new_password***
Description	Set or change the password for an account.
Parameters	***old_password***: enter the old password ***new_password***: enter the new password

Command	passwdchk
Synopsis	passwdchk user/admin [on/off]
Description	Review or set password checking for an account. Show or change the setting of password check for an account.
Parameters	[on/off]: enable or disable the password check

Command	paswdmail
Synopsis	passwdmail [-s ***account***]/[send]/[off]
Description	When enabled, the email account to which the password reminder should be sent to is displayed. When disabled, off is displayed. Only one of the three options can be specified at a time.
Parameters	[-s ***account***]: enable and set the mail account [send]: send the mail [off]: disable the function

Command	logout
Synopsis	logout/quit/bye/exit
Description	Log out the current user and return to the user name prompt.

Command	autologout
Synopsis	autologout [**x**min/off]
Description	Review or set the logout timer.
Parameters	**x**min: time out value off: turn off the auto logout function

Command	forward
Synopsis	forward [on/off]
Description	Show or change the setting of forwarding control.
Parameters	[on/off]: enable or disable the forwarding

4.9.4 System information

Command	ctlname
Synopsis	ctlname ctl**x** ***controller_name***
Description	Set the controller name.

Command	sysname
Synopsis	sysname ***system_name***
Description	Set the system name.

Command	ctllist
Synopsis	ctllist ctl**x** [-r]
Description	List the controller-related information.
Parameters	[-r] (for redundant controller only): Show internal controller status

4.9.5 Miscellaneous

Command	restart
Synopsis	restart [-h] [-c ctl**x**] [-b] [-e]
Description	Restart or halt the controller.
Parameters	[-h]: halt without restart [-c ctl**x**] (for redundant controller only): restart only one controller [-b] (for redundant controller only): effective for both controllers [-e]: effective for all external enclosures

Command	beeper
Synopsis	beeper *on/off/mute*
Description	Review or set the beeper.

Command	fwupdate
Synopsis	fwupdate ***image.bin*** [-b] [-c ctl**x**]
Description	Upload the firmware image or update the boot code with the file, image.bin.
Parameters	[-b]: update boot code [-c ctl**x**] (for redundant controller only): target controller to update

Command	fwupdateprog
Synopsis	fwupdateprog [-c ctl**x**]
Description	List the current firmware update progress.
Parameters	[-c ctl**x**] (for redundant controller only): target controller to get firmware update progress

Command	batterylist
Synopsis	batterylist ctl**x**
Description	List the status of the battery installed in a controller.

Command	ctldst
Synopsis	ctldst on/off
Description	Enable or disable the detailed self test of controller during start-up.

Command	diagdump
Synopsis	diagdump ***diag.bin***
Description	Export extensive diagnostics information from the controller to a file.

Command	nandflash
Synopsis	nandflash primary/secondary
Description	Show the current status of the on-board NAND flash chips.

Command	bbmcontrol
Synopsis	bbmcontrol on/off
Description	Enable or disable battery backup support.

Command	memtest
Synopsis	memtest on/off
Description	Enable or disable memory testing during system boot-up.

4.10 Miscellaneous Utilities

4.10.1 Lookup RAID systems

Command	raidlookup
Synopsis	raidlookup
Description	Search all RAID systems on the local network and list the following information of each RAID system: controller IP address, system model name, system name, firmware version, and beeper alarm status.

4.10.2 Turn on/off CLI script mode

Command	scriptmode
Synopsis	scriptmode [on/off]
Description	Turn on or off the CLI script mode.

4.10.3 Get command list and usage

Command	help
Synopsis	help [***class_name***/***command***]
Description	help: list the name of all classes. help ***class_name***: list commands in the specified class. help ***command***: display the full documentation.

4.11 Configuration shortcuts

4.11.1 RAID quick setup

Command	raidquick
Synopsis	raidquick [-r ***raidlevel***] [-i ***initopt***] [-s ***spare_no***]
Description	Initialize RAID configurations and LUN mapping according to the specified.
Parameters	[-r ***raidlevel***]: RAID level [-i ***initopt***]: initialization method [-s ***spare_no***]: the number of global spare disks.

4.11.2 Performance profile

Command	perfprofile
Synopsis	perfprofile [avstream/maxiops/maxthruput/off]
Description	Select the performance profile to apply
Parameters	[avstream/maxiops/maxthruput/off]: AV application, maximum IO per second, maximum throughput, or off.

4.12 Snapshot

Command	svpcreate
Synopsis	svpcreate pdevice sdevice
Description	Create a snapshot volume pair.
Restrictions	pdevice and sdevice must not be a private virtual disk. sdevice must not be used by any LUN. pdevice and sdevice must not be in faulty and regular initialization state. The capacity of sdevice must be greater than 10% of the capacity of pdevice.

Command	svpdelete
Synopsis	svpdelete pdevice
Description	Delete a snapshot volume pair.
Restrictions	There must be no snapshot volume on the volume pair.

Command	svolcreate
Synopsis	svolcreate pdevice svol**x** [-n **name**]
Description	Create a snapshot volume.
Parameters	[-n **name**]:The name of a snapshot volume.
Restrictions	Primary and secondary volume of snapshot volume pair must not be in faulty state. All snapshot volume of the same primary volume must not be in the restoring state. There must be no existed svol**x**.

Command	svoldelete
Synopsis	svoldelete svol**x** [-f]
Description	Delete a snapshot volume.
Parameters	[-f]: force to delete LUN mapping

Command	svset
Synopsis	svset pdevice/all [-p ***percentage***]
Description	Set a snapshot volume pair option.
Parameters	[-p ***percentage***]: set the threshold for overflow alert

Command	svolname
Synopsis	svolname svol***x name***
Description	Set snapshot volume name.

Command	svpimport
Synopsis	svpimport pdevice sdevice
Description	Import snapshot volumes.

Command	svimportlist
Synopsis	svimportlist
Description	List snapshot volume pairs on virtual disks.

Command	svlist
Synopsis	svlist pdevice/all
Description	List snapshot volume pairs

Command	svrestore
Synopsis	svrestore svol**x**
Description	Restores a primary volume to a snapshot volume.

Command	svspare
Synopsis	svspare add/remove dg**x**ld**y**/vol**y**/jbd**y**
Description	adds or removes a spare COW volume.

Chapter 5: Advanced Functions

5.1 Multi-Path IO Solutions

5.1.1 Overview

Multi-path IO allows a host computer to access a RAID system over multiple paths for enhancing system availability and performance. The RAID system supports multi-path IO either with the bundled proprietary software or by the native multi-path IO software of the operating systems.

The following RAID systems support multi-path IO solutions:

- 4Gb/s FC-SAS/SATA RAID system
- 3Gb/s SAS-SAS/SATA RAID system

The single-controller systems support the following operating systems:

- Windows 2003 Server 32-bit/64-bit OS (PathGuard)
- Linux with 2.6.x series kernel, like SLES 9/10, RHAS 4/5, RHEL 4/5 (Device Mapper multi-path driver).
- Solaris 10 OS (MpxIO, Multiplexed I/O)
- MAC OS X (default driver)
- VMWare ESX (default driver)

The dual-controller systems support the following operating systems:

- Windows 2003 Server 32-bit/64-bit OS (PathGuard)
- Linux with 2.6.x series kernel, like SLES 9/10, RHAS 4/5, RHEL 4/5 (Device Mapper and proprietary multi-path driver).

For the updated interoperability list and the bundled multi-path software, please contact your supplier.

5.1.2 Benefits

Below are the summarized benefits of the multi-path IO solution:

- Higher availability

With redundant paths, the failure of single path will not result in corruption of the whole system, and the applications can continue to access the storage devices without being aware of the path failures. This highly enhances the availability of the whole system.

- Higher performance

The performance of single logical device will not be limited to the upper bound of bandwidth provided by single path, and it is improved by aggregating the bandwidth of multiple paths. It also outperforms host-

side software RAID0 because RAID0 forces I/O to be truncated into data stripes, resulting in overhead and limited size of per-transaction data transfer.

- Higher bandwidth utilization

With statically assigning paths to logical devices on a controller, the bandwidth of all connections cannot be fully utilized if the loading on different logical devices is uneven. By transferring data over all paths, bandwidth utilization is more efficient, and ROI is improved.

- Easier management

With dynamic load balancing, the users need not to worry about either bandwidth planning during the installation or the reconfiguration for performance tuning. When there is new HBA or new connection is added, the bandwidth created can be utilized easily. Therefore, MPIO largely reduces the management efforts and the TCO (Total Cost of Ownership).

5.1.3 Configuring MPIO Hosts and RAID Controller

A path is defined as the link from host to a virtual disk presented by the RAID controller, and it includes the HBA, cables, and optionally a storage switch. To build multiple I/O paths, there have to be multiple links between the host computer and the RAID system, and the virtual disks in the RAID system have to be exported to multiple host-interface ports. The multi-path software on the host computer can access the virtual disks through any of the exported LUNs over the links. Because multiple HBAs (or multiple ports on single HBA) on a host computer are required to access the same set of LUN mappings, grouping these HBAs into a host group and using symmetric storage presentation for exporting LUNs would it ease your configuration tasks.

If directly attaching the host-interface ports to the HBAs, you can easily know the number of paths for single virtual disk by counting the physical links. But if a switch is used to build a fabric, you need to multiply the number of HBA ports and the number of host-interface ports of the controller to derive the number of paths. For example, if a host has three HBA ports connecting to a switch, which links to a RAID system with four host-interface ports, there will be twelve paths for the host to the RAID system.

For regular operating systems, a path is perceived as a physical disk, and accessing a LUN through different paths simultaneously without multi-path software could cause data corruption. It is the multi-path software to scan all detected physical disks (paths) and map the physical disks to single logical disk (MPIO disk) if these physical disks present consistent information to indicate that they belong to the same virtual disk. The applications then can access the LUN via the MPIO disk.

After completing the physical connections between hosts and RAID systems, please follow the steps below:

1. Create virtual disks, like JBOD disks, logical disks, and volumes
2. Choose symmetric storage presentation method
3. Add all HBA ports (with WWPN or SAS address) to the hosts in the controller
4. Selectively add hosts (HBA ports) to a host group (HG)
5. Export virtual disks to LUNs for the host group (HG)
6. Repeat the previous two steps for each host computer and host group

The hosts mentioned in this manual and the user interfaces of the RAID systems refer to the HBA ports on the host computers, and host groups refer to a group of HBA ports. For example, a host computer with two dual-port HBAs is perceived as four individual hosts by the RAID controller. Exporting a virtual disk to a host or a host group will allow the HBA port or the group of HBA ports to access the virtual disks from any of the host-interface ports in the RAID system.

NOTE

1. Because a LUN is not accessible during regular initialization, install the MPIO driver after the regular initialization is done or use background initialization.
2. Use MPIO management utility to verify that all disk devices and paths are recognized by the MPIO software.
3. Go to Section 5.2 when using MPIO with redundant-controller systems.

Bellow is the guideline and example to set up the hosts and host groups when using multi-path IO solutions:

- **Independent MPIO Hosts Computers**

For independent (non-clustered) host computers sharing single RAID system, the storage should be partitioned and accessed independently by the host computers. One host group should be created for each host computer, and the host group should include all HBA ports on the host computer. So, each host computer has LUN mappings of its own, and it can see its LUN mappings from all HBA ports and paths.

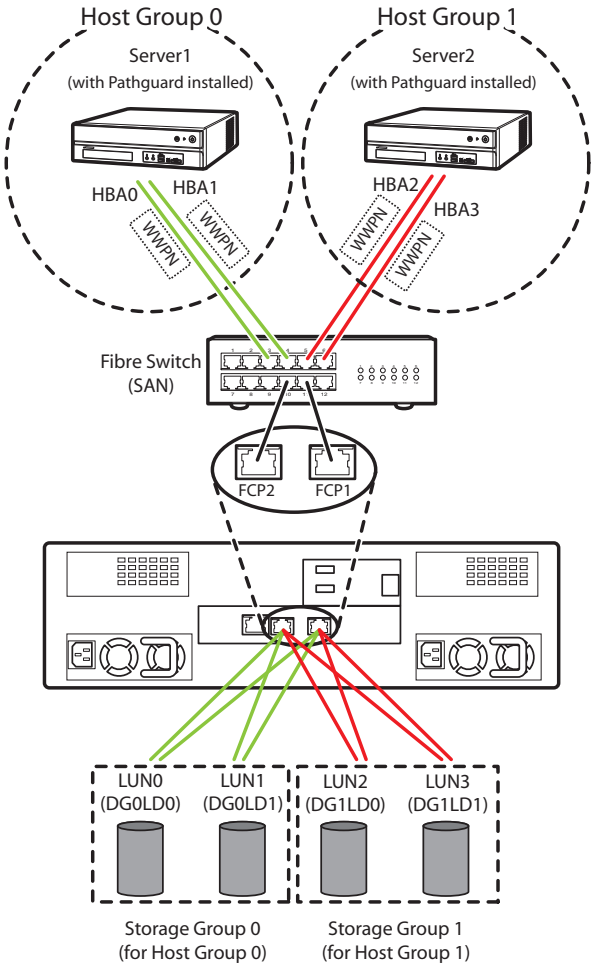


Figure 5-1 Dual independent MPIO hosts

Figure 5-26 illustrates two independent servers sharing single RAID system with multi-path I/O. Each server sees two LUNs (DG0LD0 and DG0LD1 for Server 1, and DG1LD0 and DG1LD1 for Server 2), each of which has two paths.

The table below shows the configuration steps for Figure 5-26.

Tasks	Instructions
Select Storage Provisioning method	RAID Management > Storage Provisioning > Symmetric

Add WWPN of HBAs to hosts	HBA0 WWPN -> Host 0 HBA1 WWPN -> Host 1 HBA2 WWPN -> Host 2 HBA3 WWPN -> Host 3
Add hosts to each host group	Host 0 and Host 1 -> Host Group 0 Host 2 and Host 3 -> Host Group 1
Map LUNs to host groups	DG0LD0 and DG0LD1 -> Host Group 0 DG1LD0 and DG1LD1 -> Host Group 1

- **Clustered MPIO Host Computers**

For clustered host computers sharing single RAID system, the storage is to be accessed simultaneously by all host computers. In such case, one host group should be created for all host computers, and a host group should include all HBA ports on all clustered host computers. So, all host computers can have the same LUN mappings from all paths.

Figure 5-27 illustrates two clustered servers sharing single RAID system with multi-path I/O. Both servers see the same two LUNs (DG0LD0 and DG0LD1), each of which has two paths.

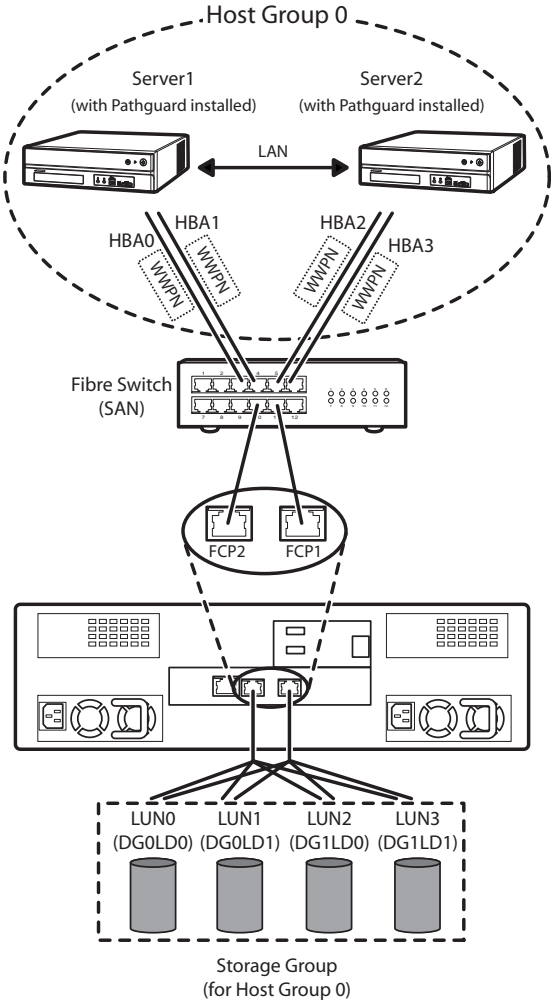


Figure 5-2 Clustered server environment

The table below shows the configuration steps for Figure 5-27.

Tasks	Instructions
Select Storage Provisioning method	RAID Management > Storage Provisioning > Symmetric

Add WWPN of HBAs to hosts	HBA0 WWPN -> Host 0 HBA1 WWPN -> Host 1 HBA2 WWPN -> Host 2 HBA3 WWPN -> Host 3
Add hosts to one host group	Host 0 and Host 1 -> Host Group 0 Host 2 and Host 3 -> Host Group 0
Map LUNs to host groups	DG0LD0 and DG0LD1 -> Host Group 0 DG1LD0 and DG1LD1 -> Host Group 0

5.1.4 Windows Multi-Path Solution: PathGuard

PathGuard is the bundled multi-path IO solution for Windows platforms, and it is based on Microsoft Multipath I/O (MPIO) framework. PathGuard consists of MPIO drivers and a web-based path manager GUI that allows you to manage MPIO configurations for multiple host computers.

The MPIO drivers include standard drivers from Microsoft and DSM (Device Specific Module) provided by the RAID system supplier.

For more information about Microsoft MPIO, please visit the link below:

http://www.microsoft.com/windowsserver2003/technologies/storage/mpio/default.mspx

The following steps are required for enabling PathGuard MPIO:

1. Complete the hardware and software setup at RAID systems
2. Install the PathGuard package to the host computer
3. Register the vendor name and model name of your RAID system to the PathGuard (optional)
4. Install the PathGuard MPIO driver
5. Reboot the host computer
6. Launch PathGuard GUI to set multi-path policies

Windows MPIO framework requires rebooting the host computer when enabling the MPIO driver on the host computer, such that the regular disk device drivers will be replaced by the MPIO disk drivers. Windows can properly detect multi-path disks only during MPIO driver installation, so reconfiguration (like adding/removing paths or LUNs) requires you to reinstall the PathGuard MPIO driver and reboot the host computer. You might need also to manually rescan the physical drives (use **Computer Management > Storage > Disk Management**) When multi-path disks are not properly detected.

- ## Install and Uninstall PathGuard

  To install the PathGuard, double click the installation file on a host computer (choose the 32-bit or 64-bit installation file according to your host system). And follow the on-screen instructions to start the installation. After the installation, you can install MPIO driver or use PathGuard GUI.

  Click the **Start > Programs > PathGuard > readme** read the online help page. To uninstall the PathGuard, click **Start > Programs > PathGuard > Uninstall PathGuard**.

- ## Register RAID system to MPIO Driver (optional)

  The MPIO driver is only applied to the RAID systems that have vendor names and model names in the PathGuard device database.

  PathGuard is delivered with predefined database, but if the MPIO driver cannot recognize your RAID systems, you may need to contact your supplier to get the updated PathGuard software or simply add the name of your RAID systems to the PathGuard database.

  A software utility can be found to do so at **Start > Programs > PathGuard > Driver > Update New Model**. After entering the vendor name and model name, press the Enter button to confirm the change. You can now re-install the MPIO driver and reboot the host computer to make it effective.

- ## Install and Uninstall MPIO Driver

  You need to install MPIO driver only on a host computer connected with RAID systems. If you use PathGuard GUI only for managing MPIO of remote sites, you need not to install the MPIO driver.

  To install the MPIO driver, click **Start > Programs > PathGuard > Driver > Install MPIO Driver**, and to uninstall it, click **Start > Programs > PathGuard > Driver > Uninstall MPIO Driver**. Reboot the host computer, and you have completed the installation or un-installation.

- ## Check the MPIO disk status on the host computer

  After the MPIO driver has been installed, you can find the *new multi-path disk device(s)* (eg. ACS82410 Multi-Path Disk Device) and the *Multi-Path Support* displayed in the following screen: **Computer Management > Device Manager**. (Right-click the **My Computer** icon on the desktop > select **Manage**)

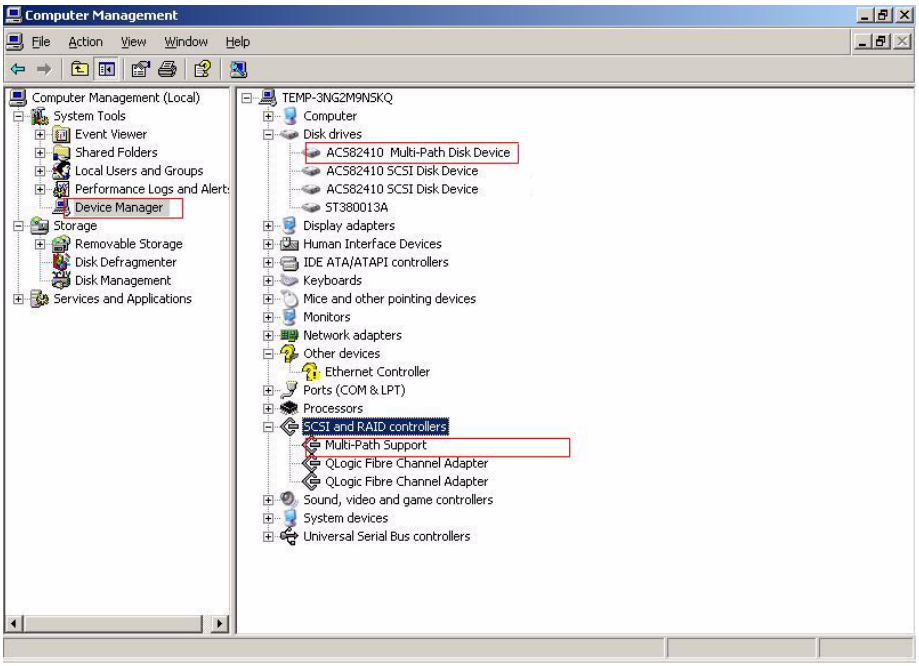


Figure 5-3 Computer Management screen: Device Manager

- ## Use the PathGuard GUI for managing MPIO disks

  You can launch the PathGuard GUI by clicking **Start > Programs > PathGuard > PathGuard GUI**. As PathGuard GUI allows you to manage multiple hosts running PathGuard MPIO drivers (either the local one or remote ones), you need to connect and login to a host before monitoring or managing its MPIO. Please follow the steps below:

  1. Click the **Connect** button
  2. Choose **Localhost** or **Remote** from the **Connect Host** drop-down menu.
  3. If **Localhost** is selected, you can click the **Login** button if you are currently using an administrator-level user account to access the local computer.
  4. If is **Remote** selected, you need to enter the name or the IP address of the remote host in the **Host Name** box. You need to also enter the name of an administrator-level user account in that remote host and the corresponding password. And you can click the **Login** button to proceed.
  5. If the authentication procedure above is done to get the access right, you can see all the MPIO disks on the login host.

- **MPIO Device Information**

When logged in, the PathGuard MPIO Utility GUI shows all connected MPIO disks.

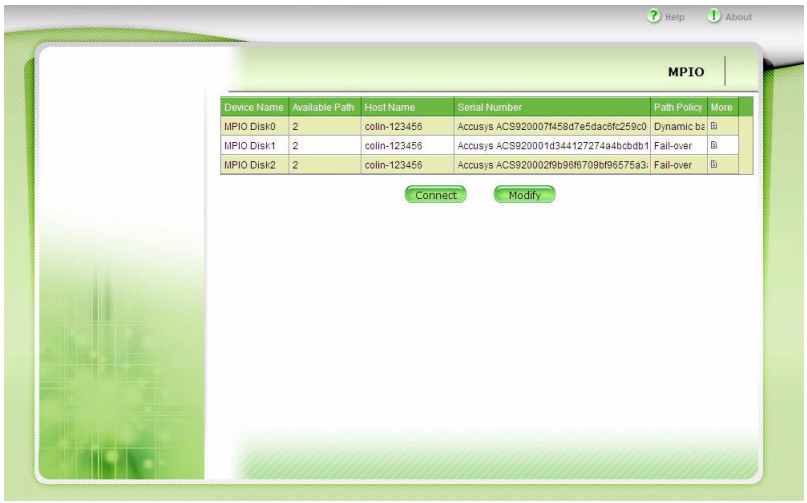


Figure 5-4 MPIO device screen

Category	Display
Device Name	MPIO Disk name
Available Path	The available number of paths on the MPIO disk
Host Name	The host name or IP address of host where the MPIO device is located
Serial Number	The RAID controller model name and serial number
Path Policy	The path policy of the selected MPIO Disk

Table 5-1 MPIO device information

- **Detailed MPIO device information**

Click to display a complete list of MPIO disk information. You will see the following details.

- Selected MPIO disk name, weight mode, and switch counter
- Physical Path ID
- Adapter Name
- LUN ID
- Path Status
- Read/Write (Byte)
- Read/Write (I/O)
- Queue

- ## Configure MPIO Policy Settings

Select the MPIO disk you want to configure, then click **Modify** to open the configurations window.

1. From the Path Policy drop-down menu, select either **Fail-over** or **Dynamic balance**.
   - If you select **Fail-over** mode, specify the preferred working path.
   - If you select **Dynamic balance** mode, specify a weight mode and switch counter.
2. Each option is described as below. Specify the settings for the selected MPIO disk.

Path Policy	**Fail-over:** The Read/Write IOs are transferred on the designated *Primary (Active)* path. The *Passive* path takes over the transfer load only when the *Primary path* is off-line. **Dynamic balance:** The Read/Write IOs on paths are transferred according to the *Weight Mode* policy.
Preferred Working Path	Select a path as the primary (active) path. The primary path takes the entire IO transfer load and the un-selected as standby path (passive).
Weight Mode	**Read/Write IOs:** Given path1 has completed x IOs, path2 has completed *y* IOs and switch counter has been set to z IOs. Whenever z Read/Write IOs have been transferred, the transferred IO Counts on each path will be checked. If x > *y* and the primary (active) path is on path1, the primary path will be switched to path2 at next IO. Vice versa, if x < *y* and current path is path2; the primary path will be switched back to path1 at next IO. **Read/Write Bytes:** Given path1 has transferred x Bytes, path2 has transferred *y* Bytes and switch counter has been set to z IOs. Whenever z Read/ Write IOs have been transferred, the transferred Read/Write Bytes on each path will be checked. If x > *y* and the primary (active) path is on path1, the primary path will be switched to path2 at next IO. Vice versa, if x < *y* and current path is path2; the primary path will be switched back to path1 at next IO.

	Command Queue: Given path1 has x IOs in queue, path2 has y IOs in queue and switch counter has been set to z IOs. Whenever z Read/ Write IOs have been transferred, the transferred Read/Write IO Queues on each path will be checked. If x > y and the primary (active) path is on path1, the primary path will be switched to path2 at next IO. Vice versa, if x < y and current path is path2; the primary path will be switched back to path1 at next IO. **Round Robin:** With switch counter set to z IOs, whenever every z Read/Write IOs have been transferred, the primary (active) path will be switched to another path.
Switch Counter	Specify a counter value for path switching. The range if from 1 to 99.

3. Click **Apply** to apply the settings on the selected MPIO disk.

5.1.5 Linux Multi-Path Solution

Native Linux multi-path I/O support has been added to the Linux 2.6 kernel tree since the release of 2.6.13, and has been back-ported into Red Hat Enterprise Linux 4 in Update 2 and into Novell SUSE Linux Enterprise Server 9 in Service Pack 2. It relies on device mapper (DM), a kernel driver framework that allows add-on drivers to be installed to the kernel to do I/O manipulation, such as logical volume management, software RAID, and also in our case, multi-path I/O.

The **dm-multipath** driver is the implementation of Linux multi-path I/O based on the device mapper driver. Together with a user-space program, **multipathd**, which when started, reads the configuration file, **/etc/multipath.conf**, to create multi-path devices at **/dev/**. It also runs as a daemon to constantly monitor and recover failed paths.

Because the DM multi-path works above the hardware layer, all HBA should work. Novell SuSE and RedHat, along with other Linux vendors, are pushing DM multi-path as the standard multi-path solution. Many RAID vendors have also adopted DM multi-path as the default multi-path solution on Linux. You may find extensive related information over the Internet.

For single-controller RAID systems, native Linux multi-path has everything you need, and the default configuration file can be used. All you need to do is to make sure the dm-multipath tool has been installed on your Linux systems (RHEL 5 requires manual installation of dm-multipath package). The sections below are examples offered for SUSE SLES 10. For redundant-controller RAID systems, in addition to the native Linux dm-multipath, you need also to install the proprietary RPM package and edit the configuration file.

- Install and start the multipathd service

(Single-Controller System)

1. Check **/etc/multipath.conf**, and if it is not there, you need to build it (see the example under **/usr/share/doc/packages/multipath-tools/multipath.conf.synthetic**).
2. To install **multipathd** into your Linux service scripts, type insserv **/etc/init.d/multipathd**.
3. To activate **multipathd** service on your Linux service scripts, type **chkconfig -a multipathd**, and the screen shows the Linux run levels at which **mulitpathd** will be turned on or off:

```
linux-go62:/ # chkconfig -a multipathd
multipathd              0:off  1:off  2:off  3:on   4:off  5:on   6:off
```

After completing the steps above, your Linux will launch **multipathd** automatically during the system boot-up. But at this moment, **multipathd** is still not started.
For Red Hat in here that is different,please type **chkconfig multipathd on.**

4. To manually start **multipathd** service, type **service multipathd start**. The screen shows:

```
linux-go62:/ # service multipathd start
Starting multipathd                                        done
```

- Uninstall and stop the multipathd service

(Single-Controller System)

1. To immediately stop the service, type service multipathd stop. But note that you have to un-mount the file system over the multi-path devices before doing so to avoid data loss.
2. To deactivate multipathd service on you system, type **chkconfig multipathd off**. This will stop the auto-start of the multipathd during the boot time.
3. To completely remove the multipathd service on you system, type **insserv -r /etc/init.d/multipathd**.

- Install and start the multipathd service

(Redundant-Controller System)

For redundant-controller systems, the Linux multi-path requires proprietary driver to recognize the controller preference to deliver optimal performance. The driver depends on the kernel version of your Linux, and below list the pre-built driver binaries:

RHEL5/32bit: mpath-xxx-x.i386-rhel5.rpm

RHEL5/64bit: mpath-xxx-x.x86_64-rhel5.rpm

RHEL5 Xen/64bit:mpath-xxx-x.x86_64xen-rhel5.rpm

SuSe10/32bit: mpath-xxx-x.i586-sles10.rpm

SuSe10/64bit: mpath-xxx-x.x86_64-sles10.rpm

If your Linux kernel cannot match the pre-built driver binaries, you may also build the binary on your own.

Below are the source RPM packages:

RHEL5: mpath-xxx-x.src-rhel5.rpm

SuSe10: mpath-xxx-x.src-sles10.rpm

1. Install the RPM by typing **rpm -ivh mpath-xxx-x.xxx-xxxx.rpm**. This not only installs the driver but also starts the multipathd service like the procedures described for the single-controller system.
2. To build a driver binary, follow the steps below:

   2.1 Type **rpm -ivh mpath-xxx-x.src-xxxx.rpm** to install the source code package

   2.2 Change working directory to **/usr/src/packages/SPECS** and type **rpmbuild -bb mpath.spec**

   2.3 Change working directory to **/usr/src/redhat/packages/RPMS/ "your ARCH"** and Type **rpm -ivh mpath-xxx-x.rpm**

3. Edit **/etc/multipath.conf** to specify the vendor names, product names, priority callout function, and hardware handler. An example is illustrated as below:

```
devices {
    device {
        vendor                  "vendorname"
        product                 "productname"
        path_grouping_policy    group_by_prio
        getuid_callout          "/sbin/scsi_id -p 0x80 -g -u -s /block/%n"
        prio_callout            "/sbin/acs_prio_alua %d"
        hardware_handler        "1 acs"
        path_checker            hp_sw
        path_selector           "round-robin 0"
        failback                immediate
        no_path_retry           queue
        rr_min_io               100
        product_blacklist       LUN_Z
    }
}
```

- **Uninstall and stop the multipathd service**

(Redundant-Controller System)

Simply type **rpm -e mpath-xxx-x**

- **Access to multi-path devices**

1. If no error message is displayed during the installation and startup of the **multipathd** service, you've successfully started the **multipathd**, and you can now go to **/dev/** to find the multi-path devices, which are named as dm-x, where x is a number assigned by the DM driver.
2. You can create partitions on **/dev/dm-x** using **fdisk** or **parted** command. To access the partitions, you need also to use **kpartx** to create DM devices in the **/dev/**.

- **Manage multipathd service**

1. To view the LUNs of the attached RAID systems, type **cat /proc/scsi/scsi**, and similar outputs are displayed as below:

```
linux-go62:/ # cat /proc/scsi/scsi
Attached devices:
Host: scsi0 Channel: 00 Id: 00 Lun: 00
  Vendor: Accusys  Model: ACS82410         Rev: 0001
  Type:   Direct-Access                    ANSI SCSI revision: 05
Host: scsi1 Channel: 00 Id: 00 Lun: 00
  Vendor: Accusys  Model: ACS82410         Rev: 0001
  Type:   Direct-Access                    ANSI SCSI revision: 05
```

2. To check if multipathd service has been activated or not, type **chkconfig --list multipathd**.
3. To check if service has been running or not, type **serivce -- status-all**.The multipathd provides several commands for configuring the paths as well as showing path and device information. Type **multipathd -k** to enter its interactive mode.
4. You may also use **multipath** command to configure, list, and remove multi-path devices.
5. To add or remove LUNS, after completing the changes to the RAID system configurations, restart the service by typing **service multipathd restart**. Modifying the configuration needs also to restart the service to make the modifications effective.
6. If you're running Linux cluster and need to have consistent multi-path device names, you need to use the **alias** option in **multipath.conf** or to use the Linux persistent binding.
   For complete information, please go to RedHat and Novell web site to find the following online documents:
   - RedHat: "Using Device-Mapper Multipath"
   - Novell SUSE: "SLES Storage Administration Guide"

5.1.6 MAC Multi-Path Solution

Mac OS X provides multi-path support on a basis since OS X 10.3.5, providing both path redundancy and load balancing. Mac OS X implements miltipathing at the target device level, and it requires that the RAID controller presents the same World Wide Node Name (WWNN) to all the host interfaces connected to the MAC systems. Please refer to • **Setting FC Worldwide Node Name on page 2-60** to select identical WWNN. After restarting the RAID system to make this change effective, then follow **5.1.3 Configuring MPIO Hosts and RAID Controller on page 5-2** to complete the LUN mapping configurations.

The Mac OS multipath I/O driver by default supports only round-robin I/O policy. With Apple Xsan software, you may set the policy to be either round-robin (rotate) or static (failover-only). For more information please visit Apple web site and read "Apple Xsan Administrator's Guide".

5.1.7 VMware ESX Server Multi-Path Solution

VMware ESX Server 2.5 or the later by default is loaded with hardware-independent multi-path drivers and management interface. After completing the RAID system configurations and attaching the RAID system to the host computer, you may use VMware Management Interface or the command, **vmkmultipath** or **esxcfg-mpth**, at Service Console to manage the paths.

There are three multi-path policy options supported:

1. **fixed** -- using user-predefined path.
2. **mru** -- using most recently used path.
3. **rr** -- using round-robin algorithm, which is available only after ESX Server 3. The first two polices are use only one active path, and move to a standby path only when the active path is down. The third policy can use all paths at the same time to deliver the best performance. You may use **esxcfg-advcfg** to set path performance parameters. The single-controller RAID system supports all the options.

When a cable is pulled, I/O freezes for approximately 30-60 seconds, until the SAN driver determines that the link is down, and failover occurs. During that time, the virtual machines (with their virtual disks installed on a SAN) might appear unresponsive, and any operations on the /vmfs directory might appear to hang. After the failover occurs, I/O should resume normally.

After changing the configuration of LUN or paths, please use **esxcfg-rescan** command to do rescan and **esxcfg-vmhbadevs** to know the mapping between device names and the LUNs.

For more information, please refer to VMware ESX Server Administration Guide and VMware ESX Server SAN Configuration Guide, or go to **http://www.vmware.com/**.

5.1.8 Sun Solaris 10 OS Multi-Path Solution

The latest Sun Solaris OS 10 has integrated Storage Multipahting software, which offers path failover and a path management utility. The single-controller RAID system is fully compliant with the software. After configuring the LUN mappings and connecting the RAID system to Solaris system, you may find multi-path devices in the device directory with their name of the following format: **/dev/dsk/c3t2000002037CD9F72d0s0**, which is largely different from non-multi-path devices, **/dev/dsk/c1t1d0s0**.

The path management utility, **mpathadm**, allows you to list paths, list LUN discovered, configure auto-failover, and control paths. Please check its man page. For more information about multi-path on Solaris, please refer to "Solaris Fibre Channel and Storage Multipathing Administration Guide", or go to Sun's online document web site: **http://docs.sun.com/**, and Sun's online forum web: **http://wikis.sun.com/**.

5.2 Multiple ID solutions

5.2.1 Overview

The multiple ID mechanism provides host transparent controller failover/ failback solution. That is, no particular software or driver is required to be installed at the host side. Howerver, a fiber switch is required. Through the connection of fiber switch, the fiber host chanel ports can provide backup for each other. 'Fcpa1' and 'fcpb1' can backup each other, so do 'fcpa2' and 'fcpb2'.

For example, if controller A fails, 'fcpb1' inherits the target ID of 'fcpa1', while 'fcpb2' inherits the target ID of 'fcpa2'. When the target ID is inherited, the lun-map under the ID is inherited as well. Now, both 'fcpb1' and 'fcpb2' have two IDs. When controller A gets failback, 'fcpb1' and 'fcpb2' disable the inherited ID before 'fcpa1' and 'fcpa2' are enabled. The procedure is delicately controlled to achieve seamless failover/ failback.

When MTID mode is selected, the topology is set to arbitration loop automatically. The fiber switch ports connected to the RAID fiber ports should be configured as public loop ports which are often denoted as FL or GL ports. The target loop ID can be changed manually to avoid conflict with initiator loop ID if a simple fiber hub is used.

At the moment, only A16-R-FS RAID system supports multiple ID solutions.

As **Figure 5-5** shows, the green and the red dotted paths are both active paths. When the green path link fails, the red dotted path will continue to access all the storage devices without interruption.

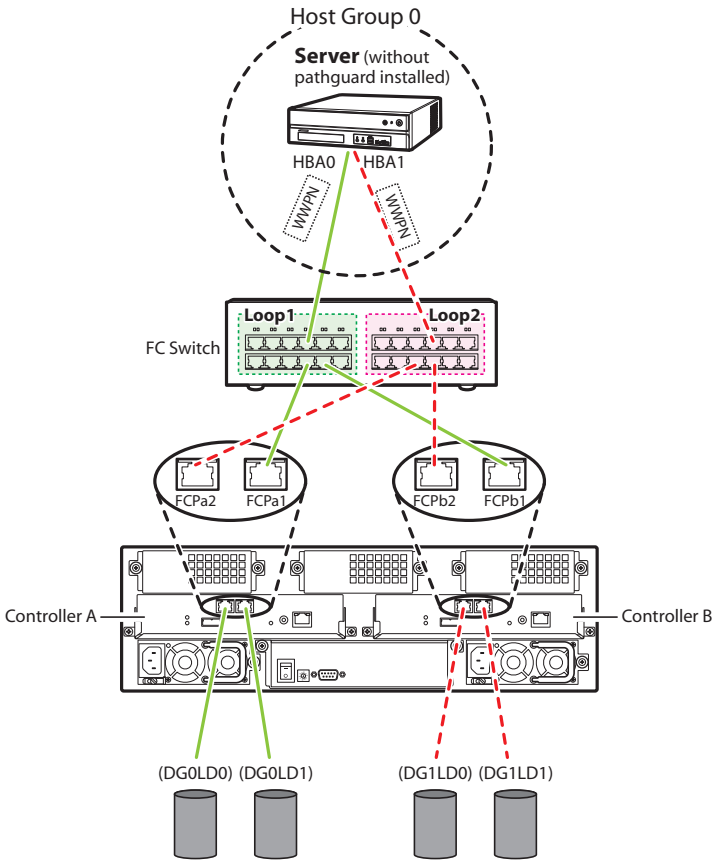


Figure 5-5 MTID environment

To set up the connection, perform these tasks in the RAID GUI:

- Create virtual volumes and specify the preferred controllers
- Specify the storage provisioning method
- Specify the LUN ID and map LUNs to fiber ports

The succeeding *Configuration Tasks* table shows the details of each configuration task according to the example given in **Figure 5-5**.

Configuration Tasks

Tasks	Instructions
Create Virtual volumes and specify the preferred controller	RAID Management > Disk Groups > Create DG0 and DG1 RAID Management > Logical Disks > Create DG0LD0 > Specify the preferred controller as **ctla** RAID Management > Logical Disks > Create DG0LD1 > Specify the preferred controller as **ctla** RAID Management > Logical Disks > Create DG1LD0 > Specify the preferred controller as **ctlb** RAID Management > Logical Disks > Create DG1LD1 > Specify the preferred controller as **ctlb**
Select Controller Failover mode	Multiple-ID
Select Storage Provisioning method	RAID Management > Storage Provisioning > Simple
Specify the LUN ID and map LUNs to fiber ports	fcpa1 -> DG0LD1 fcpa2 -> DG0LD0 fcpb1 -> DG1LD1 fcpb2 -> DG1LD0

5.3 Redundant Controller

5.3.1 Overview

Redundant controller is a high-availability solution for ensuring system availability against controller failure and for improving the performance by doubling the I/O processing power. A redundant-controller system incorporates two active-active controllers that can service I/O concurrently and take over each other if any controller fails. This section introduces basic concept of redundant-controller operations.

- **Dual controller configuration and status synchronization**

The two controllers synchronize with each other by the dedicated high-speed Redundant-controller Communication Channels (RCC) on the system backplane. The synchronization allows a controller to know the configurations and status of the peer controller, such that it can take over the jobs of a failed peer controller. It also allows you to access any one controller to monitor the status of the system or to do configurations for both controllers.

- **Mirrored write cache**

A controller caches data in the memory for performance when the delay-write option is turned on. To ensure that the cached data can be retained, data written to one controller is also forwarded to the peer controller. The RCC also serves as the path of data forwarding for mirroring write cache. You may also disable the write cache mirroring by the UI (see Mirrored Write Cache Control option on Section 2.7.15).

- **Controller failover and failback**

Both controllers monitor each other by periodic heartbeat signaling packets exchanged over the RCC. If a controller detects that the RCC link is offline or the heartbeat signal is not received within a period of time, it will power off the peer controller and start the controller failover procedure. The I/O access to the faulty controller will be redirected to the surviving controller, and the background tasks will also be continued by the surviving controller.

When the faulty controller is replaced by a new controller, the surviving controller will negotiate with the replacement controller to perform the controller failback procedure. The replacement controller will get synchronized with the surviving controller to learn the latest status and configurations. After that, the surviving controller will stop servicing the I/O for the peer controller, and the replacement controller will take back all the background tasks.

- **Multi-path IO (MPIO) and controller preference**

When using SAS host interface or using FC host interface without a switch, the redundant-controller system requires MPIO driver installed at host side

for I/O redirection during controller failover and failback. You have to symmetrically export the same LUN mappings for all host-interface ports, such that a virtual disk can be seen by all I/O paths of both controllers and controller failover/failback can work. After LUN configurations and host-interface connections are done, please install the MPIO drivers provided by your RAID system supplier to set up the redundant-controller configurations.

The redundant-controller solution is compliant with T10 TPGS (Target Port Group Standard) architecture. When a virtual disk is created, one of the two controllers is assigned to it as the preferred controller (see the Preferred Controller option in Section 2.6.2, 2.6. 4, and 2.6.5 for creating JBOD disk, logical disk, and volume, respectively). When the I/O paths from host computers to the virtual disk are available and the preferred controller is online, the MPIO driver will dispatch the I/O to the paths of the preferred controller for the virtual disk.

- **Owner controller and preferred controller**

The controller implements the ALUA (Asymmetric Logical Unit Access) algorithm to ensure that only one controller is allowed to access a virtual disk. The controller that controls a virtual disk is the owner controller of the virtual disk. When both controllers are healthy and all paths are online, the owner controller is the same as the preferred controller. There are two possible cases that the preferred controller loses the ownership of a virtual disk to the peer controller:

1. If a controller fails, the survival controller will take over the ownership of all virtual disks of the faulty controller.

2. When all the paths to a controller are disconnected, the MPIO driver will force the virtual disks to transfer to the other controller.

NOTE

To get best performance, make all LDs in a DG have the same preferred controller, and evenly distribute DGs between the two controllers.

The preferred controller is specified when a virtual disk is created, and it can be changed later by users (see the Preferred Controller option in Section 2.6.2, 2.6. 4, and 2.6.5 for modifying JBOD disk, logical disk, and volume, respectively). But the owner controller is changed dynamically according to the current path and controller status.

NOTE

Once the a virtual disk has been exported to host as a LUN on a controller, the owner controller can be changed only after restart the controller, and the Change owner controller immediately option is not displayed.

- **Single-controller mode in redundant-controller system**

If a redundant-controller RAID system is powered up with only one controller installed, the system will be operating in the single-controller mode, and there is no event or beeper alert because of the absence of the peer controller. But if the other controller is installed, the system will be operating in redundant-controller mode.

While enabling the mirror write cache protects the data integrity, disabling this option may cause data loss when the controller is failover but allows better write performance. For the purpose of data protection, it is suggested to turn this option on.

5.3.2 Controller Data Synchronization

When running in a redundant environment, two controllers will automatically synchronize the configuration data, event logs, task progress data, system time, and firmware. See further details as described below.

- **Configuration data**

The controller's configurations and states are synchronized between two controllers. There are two copies of one identical configuration data in the two controller. Updating the two copies of configuration data should be considered as an atomic operation.

- **Event logs**

The event logs are mirrored between controllers. Users can view the event logs even one of controllers is failed. The SMTP and SNMP configuration will be also the same across the master and slave controllers. Should the master controller is failed to send the event notification, the system will try to send it through the slave controller, and vice versa.

- **Task progress data**

The task progress data of a controller's background task will be synchronized to the peer controller. If one controller fails, the other can resume the background task of the failed controller.

- **Time**

Two controllers will keep syncing the Real Time Clock (RTC) in a fixed period of time.

- **Firmware**

The redundant controller system must have the two controllers to be operated in the same firmware version. There are four scenarios for firmware version update.

  - Boot State Update

Upon system boot, if the firmware version and boot code of the two controllers are unmatched, the system will have prompt text shown on

the LCD. The user needs to select the target version or boot code through the LCD menu interface.

- Failback State Update

When the backup controller's firmware version is different with the survival controller, the survival controller will automatically synchronize the firmware to the backup controller to make the two controllers with the same firmware version. The user needs to confirm the firmware update by pressing the button on the LCD panel to continue the automatic synchronization.

- Normal State Update

The normal state indicates that two controllers are normally in use. When the system receives a firmware update command, it first updates the primary flash and then the secondary flash on both controllers. After that, the system will execute non-interruptible firmware update to make the redundant-controller system always remains online.

For example, once the firmware update is executed on controller A, all the LUN mappings will be shifted from controller B to controller A. Then the controller B restarts automatically. When the controller B is completed with the firmware update, all the LUN mappings will be shifted from controller A to controller B. The controller A then restarts automatically.

- Degraded State Update

When the system is operating in a degraded state, users simply perform the firmware update on a single controller. However, when the failed controller is replaced, the system will automatically synchronize the firmware to the replacement controller.

5.3.3 Redundant-Controller System Configuration with MPIO

- **Active-Active Redundant Single MPIO Host (Dual Channel)**

As **Figure 5-6** shows, the redundant RAID system is operating in a single MPIO host environment using the symmetric storage provisioning method. The access channel is established via two fibre ports, fcpa1and fcpb1. The redundant paths of two LUNs are also established by mapping them across two fibre ports.

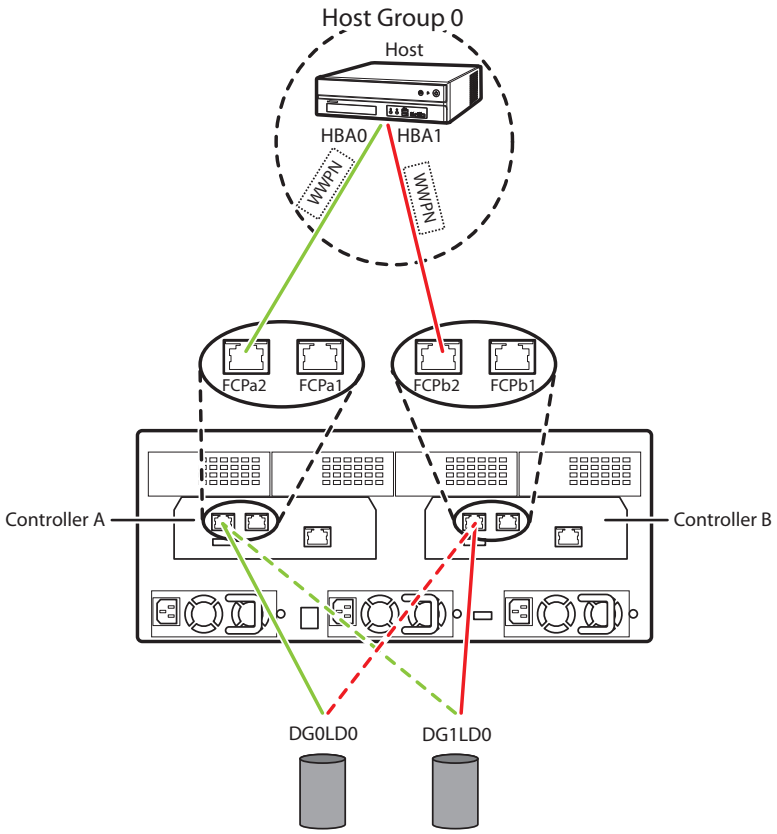


Figure 5-6 Redundant Single MPIO host (dual channel)

To set up the connection, perform these tasks in the RAID GUI:

- Create DG0LD0 with preferred controller A; create DG1LD0 with preferred controller B
- Specify the storage provisioning method
- Assign the WWPN for the HBAs in the server hosts, and group them into a host group
- Bind the two logical disks to the host group

In this configuration, for DG0LD0, the green path is the active path while the red path is the standby path, when the green path fails, the link transfroms and access will be continued by the red dotted path; for DG1LD0, the condition is reversed. Please check other similar description in section 5.3.

The *Configuration Tasks* table shown below details each configuration task according to the example given in **Figure 5-6**.

Configuration Tasks (Using Symmetric Provisioning method)

Tasks	Instructions
Create Virtual volumes and specify the preferred controller	RAID Management > Disk Groups > Create DG0 and DG1 RAID Management > Logical Disks > Create DG0LD0 > Specify the preferred controller as **ctla** RAID Management > Logical Disks > Create DG1LD0 > Specify the preferred controller as **ctlb**
Select Storage Provisioning method	RAID Management > Storage Provisioning > Symmetric
Add WWPN of HBAs to hosts	HBA0 WWPN -> Host 0 -> Host Group 0 HBA1 WWPN -> Host 1 -> Host Group 0
Map LUNs to host groups	DG0LD0 and DG1LD0 -> Host Group 0

Users can also use the simple provisioning method to establish the connections. The steps are given below.

Configuration Tasks (Using Simple Provisioning method)

Tasks	Instructions
Create Virtual volumes and specify the preferred controller	RAID Management > Disk Groups > Create DG0 and DG1 RAID Management > Logical Disks > Create DG0LD0 > Specify the preferred controller as **ctla** RAID Management > Logical Disks > Create DG1LD0 > Specify the preferred controller as **ctlb**
Select Storage Provisioning method	RAID Management > Storage Provisioning > Simple
Specify the LUN ID and map LUNs to fiber ports	fcpa2 -> DG0LD0 fcpa2 -> DG1LD0 fcpb2 -> DG0LD0 fcpb2 -> DG1LD0

- **Active-Active Redundant Single MPIO Host (Quad Channel)**

As **Figure 5-7** shows, the redundant RAID system is operating in a single MPIO host environment using the symmetric storage method. The access channel is established via four fibre ports, fcpa1, fcpa2, fcpb1, and fcpb2. The redundant paths of all LUNs are also established by mapping them across four fibre ports.

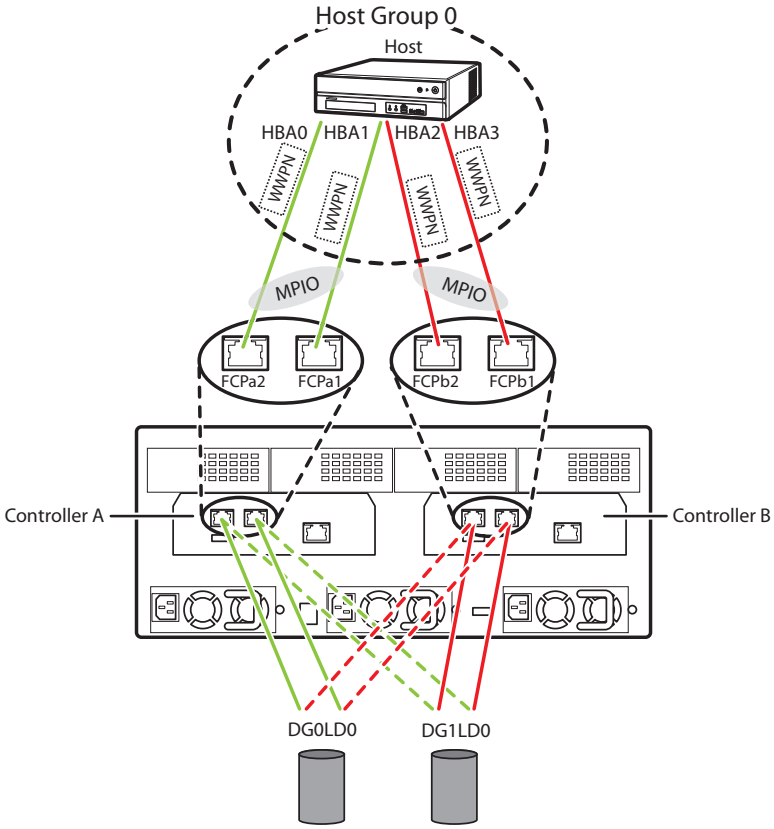


Figure 5-7 Redundant Single MPIO host (quad channel)

In this configuration, for DG0LD0, the green path is the active path while the red path is the standby path, when the green path fails, the link transfroms and access will be continued by the red dotted path; for DG1LD0, the condition is reversed.

The steps to configure the LUN mappings is the same as the dual channel configuration of redundant single MPIO host. See the following *Configuration Tasks* table for the quad channel configuration according to the example given in **Figure 5-7**.

Configuration Tasks

Tasks	Instructions
Create Virtual volumes and specify the preferred controller	RAID Management > Disk Groups > Create DG0 and DG1 RAID Management > Logical Disks > Create DG0LD0 > Specify the preferred controller as **ctla** RAID Management > Logical Disks > Create DG1LD0 > Specify the preferred controller as **ctlb**
Select Storage Provisioning method	RAID Management > Storage Provisioning > Symmetric
Add WWPN of HBAs to hosts	HBA0 WWPN -> Host 0 -> Host Group 0 HBA1 WWPN -> Host 1 -> Host Group 0 HBA2 WWPN -> Host 2 -> Host Group 0 HBA3 WWPN -> Host 3 -> Host Group 0
Map LUNs to host groups	DG0LD0 and DG1LD0 -> Host Group 0

- **Active-Active Redundant Dual Independent MPIO Hosts**

As **Figure 5-8** shows, the redundant RAID system is operating in a dual independent MPIO hosts environment using the selective storage method. All LUNs are formed into storage groups, used to bind the host groups across four fibre ports.

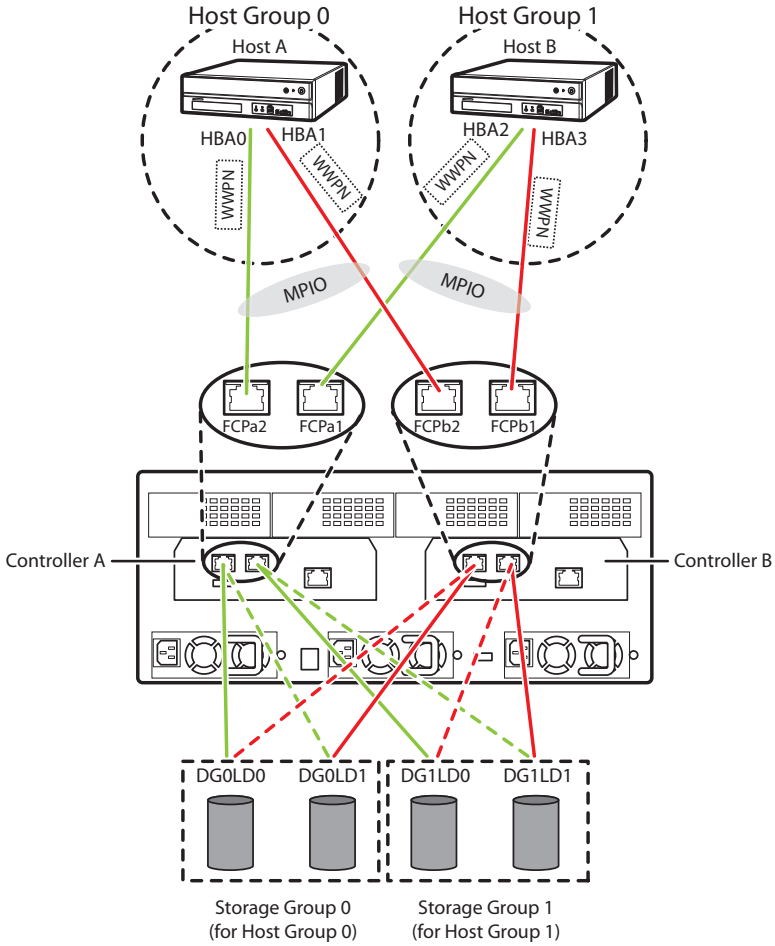


Figure 5-8 Redundant Dual Independent MPIO hosts

To set up the connection, perform these tasks in the RAID GUI:

- Specify the storage provisioning method
- Assign the WWPN for the HBAs in the server hosts
- Define the host group to which the server host belongs to
- Create storage groups for LUNs
- Bind storage groups to each host group across four fibre ports

In this configuration, for DG0LD0 and DG0LD1, the green path is the active path while the red path is the standby path, when the green path fails, the link transfroms and access will be continued by the red dotted path; for DG1LD0 and DG1LD1, the condition is reversed.

In this configuration, each LUN is mapped to all fibre ports, one is active path and the other is standby path. The *Configuration Tasks* table shown below details each configuration task according to the example given in **Figure 5-8**.

Configuration Tasks

Tasks	Instructions
Create Virtual volumes and specify the preferred controller	RAID Management > Disk Groups > Create DG0 and DG1 RAID Management > Logical Disks > Create DG0LD0 > Specify the preferred controller as **ctla** RAID Management > Logical Disks > Create DG0LD1 > Specify the preferred controller as **ctlb** RAID Management > Logical Disks > Create DG1LD0 > Specify the preferred controller as **ctla** RAID Management > Logical Disks > Create DG1LD1 > Specify the preferred controller as **ctlb**
Select Storage Provisioning method	RAID Management > Storage Provisioning > Selective
Add WWPN of HBAs to hosts	HBA0 WWPN -> Host 0 HBA1 WWPN -> Host 1 HBA0 WWPN -> Host 2 HBA1 WWPN -> Host 3
Add hosts to each host group	Host 0 and Host 1 -> Host Group 0 Host 2 and Host 3 -> Host Group 1
Assign LUNs to storage groups	DG0LD0 and DG0LD1 -> Storage Group 0 DG1LD0 and DG1LD1 -> Storage Group 1
Bind host groups and storage groups to the fibre ports	Storage Group 0 bound to Host Group 0 -> fcpa2 and fcpb2 Storage Group 1 bound to Host Group 1 -> fcpa1 and fcpb1

- **Active-Active Redundant Dual MPIO Clustering Hosts (With Fibre/SAS switch)**

As **Figure 5-9** shows, the redundant RAID system is operating in a clustering environment with dual MPIO hosts and two FC/SAS switches. Users should be notified that the number of FC/SAS switches, hosts, and controller must be the same when working in a clustering environment.

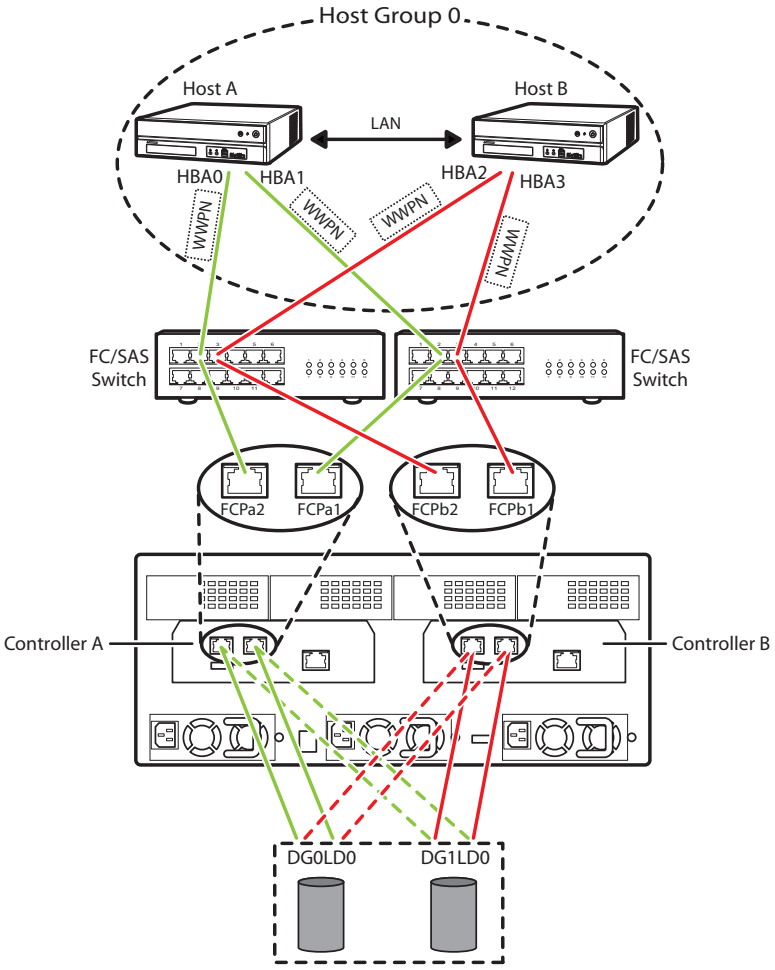


Figure 5-9 Dual clustering MPIO hosts

In this configuration, for DG0LD0, the two green solid path is the active path by controller A while the two red dotted path is the standby path by controller B; for DG1LD0, the condition is reversed.

Before proceeding with the following configuration tasks, ensure the FC/SAS switches are used to establish the connections between the hosts and the redundant RAID system. Then perform the GUI configuration tasks as described in the following *Configuration Tasks* table.

Configuration Tasks

Tasks	Instructions
Create Virtual volumes and specify the preferred controller	RAID Management > Disk Groups > Create DG0 and DG1 RAID Management > Logical Disks > Create DG0LD0 > Specify the preferred controller as **ctla** RAID Management > Logical Disks > Create DG1LD0 > Specify the preferred controller as **ctlb**
Select Storage Provisioning method	RAID Management > Storage Provisioning > Symmetric
Add WWPN of HBAs to hosts	HBA0 WWPN -> Host 0 HBA1 WWPN -> Host 1 HBA0 WWPN -> Host 2 HBA1 WWPN -> Host 3
Add hosts to each host group	Host 0, Host 1, Host2, and Host 3 -> Host Group 0
Map LUNs to host groups	DG0LD0 -> Host Group 0 DG1LD0 -> Host Group 0

- **Active-Passive Redundant Single MPIO Host (Dual Channel)**

  In the active-passive mode, one controller is active to process all I/O requests, while the other is idle in standby mode ready to take over I/O activity should the active primary controller is failed.

  As **Figure 5-10** shows, the controller A serves as an active role, and the controller B as a standby role. Two LUNs are both mapped to two fiber ports, fcpa2 and fcpb2. For all LUNs, the green path is the active path to the controller A, and the red path is the standby path to the controller B.

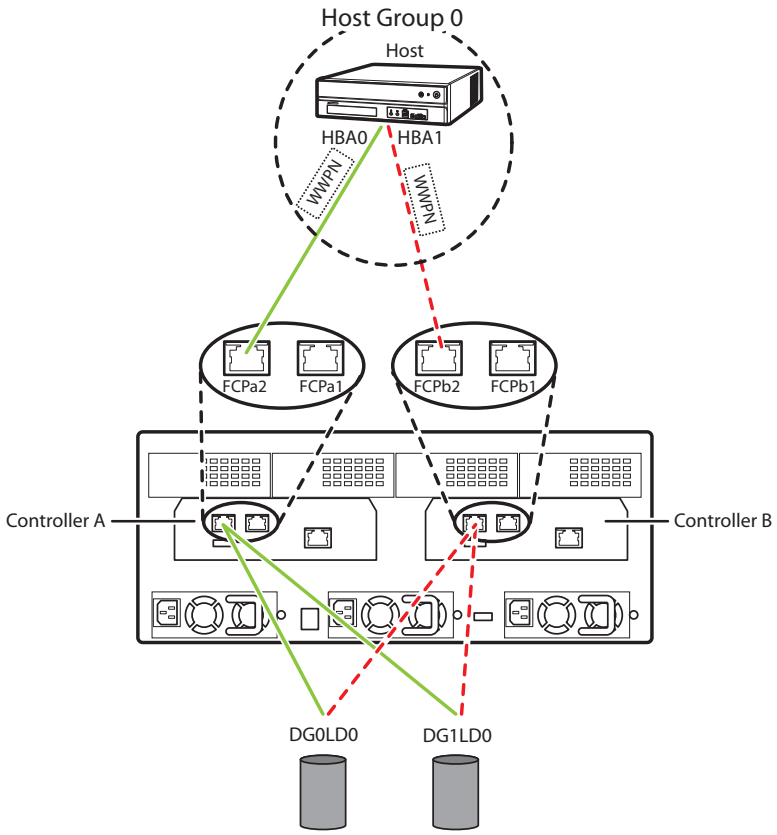


Figure 5-10 Active-Passive Redundant Single MPIO host

The steps to set up the active-passive and active-active connections are almost the same. You simply need to specify all the LUNs to the same preferred controller in the RAID GUI.

The *Configuration Tasks* table shown below details each configuration task according to the example given in **Figure 5-10**.

Configuration Tasks

Tasks	Instructions
Create Virtual volumes and specify the preferred controller	RAID Management > Disk Groups > Create DG0 and DG1 RAID Management > Logical Disks > Create DG0LD0 > Specify the preferred controller as **ctla** RAID Management > Logical Disks > Create DG1LD0 > Specify the preferred controller as **ctla**
Select Storage Provisioning method	RAID Management > Storage Provisioning > Symmetric
Add WWPN of HBAs to hosts	HBA0 WWPN -> Host 0 -> Host Group 0 HBA1 WWPN -> Host 1 -> Host Group 0
Map LUNs to host groups	DG0LD0 and DG1LD0 -> Host Group 0

5.3.4 Controller and Path Failover/Failback Scenarios

By incorporating with the MPIO driver, the access to any virtual disk can be continued when one of the controller is failed. Two principles should be cared for proper operation:

1. MPIO driver must be installed in the hosts.
2. All virtual disks must be mapped to the host across two controllers.

Path Failover Across Controllers

The paths to a VD on its preferred controller are called active paths, while the paths on the counterpart are called standby paths. When all active paths are failed, the MPIO driver directs the traffic to standby paths. **Figure 5-11** depicts the scenario.

NOTE

The path failure may be caused by pure path failure or controller failure.

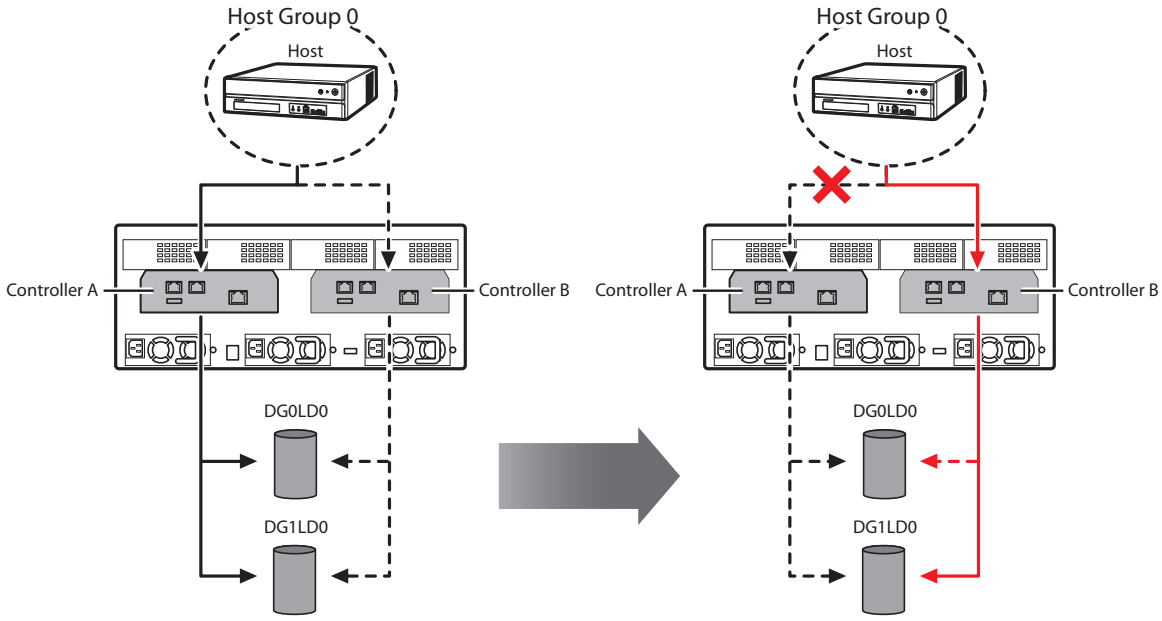


Figure 5-11 Controller failover

Path Failback Across Controllers

When any active path is restored, the MPIO driver routes the traffic back to the active path automatically. No user intervention is needed for the path failback process.

- ## Controller Failover and Failback Scenarios

When doing the controller failover and failback in the redundant-controller systems, the two controllers must meet the following hardware and software requirements:

Hardware:

1. Both controllers are of the same model and PLD version
2. Same number and model of daughter boards installed on both controllers
3. Same BBM (battery backup module) number and state
4. Same memory size

Software:

Some software requirements can be updated synchronously during the controller failback. Users need to check and confirm the pop-up message shown on the LCD panel so that the automatic synchronization can continue.

1. Same boot code
2. Same firmware version
3. Same BBM control options
4. Same enclosure serial number

Controller Failover

When one of two controllers is failed, the survival controller turns off the power of the failed one, taking over all interrupted tasks. The host I/O is redirected to controller B by MPIO driver. **Figure 5-12** shows the path switching while controller failover.

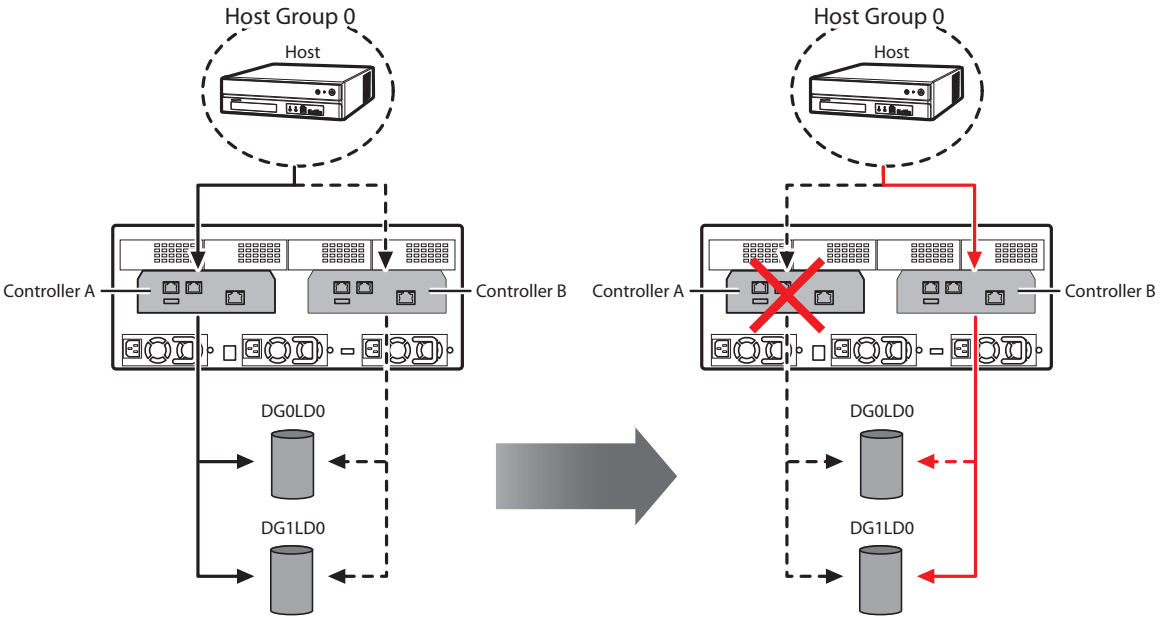


Figure 5-12 Controller failover scenario

Normally, the heartbeat LED on each controller board is flashing periodically and the system keeps syncing state messages shown on the GUI to identify the controller is alive. When a heartbeat LED does not flash anymore, or the state message cannot be synced, the controller will be regarded as failed.

NOTE

When the heartbeat LED of both controllers are flashing, users are allowed to hot remove any one controller.

Controller Failback

If a system is in the controller failover mode, the survival controller will take over the failed controller's job and process its own job. When a healthy replacement controller is installed, the system will proceed the failback process. The survival controller will return the failed controller's job and sync all states and configuration to the failback controller.

When the redundant mode is established, the heartbeat LED of the failback controller flashes. Never remove or power down (through the

GUI) the survival controller before the failback controller heartbeat LED starts flashing.

NOTE

1. Only the tasks belong to the preferred controller will be returned to the failback controller. If you have changed the preferred controller for tasks to the survival controller, the survival controller then takes the ownership of those tasks. For more information about preferred controller, see **Owner controller and preferred controller** on page 5-22.
2. The replacement must be exactly the same controller as the surviving one, as mentioned previously.

- ## GUI Notification

When one of the controller is failover, the following notification message will be displayed and provide the link to the backup controller. Click '**Go to peer controller's GUI**' to view or configure settings.

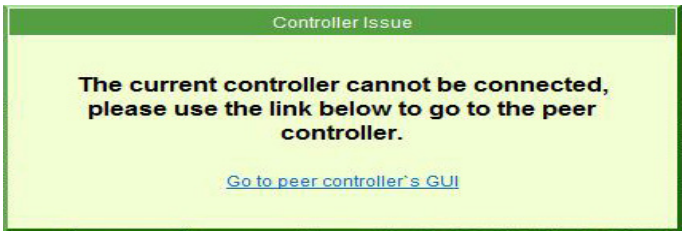

Controller Issue
The current controller cannot be connected, please use the link below to go to the peer controller.
Go to peer controller's GUI

Figure 5-13 Controller failover and the page redirection message

When a controller is failback, a pop-up dialog box appears to notify users that the system is doing failback (GUI screen is polling every 15 seconds). Users can click the **OK** button when the failback process is finished.

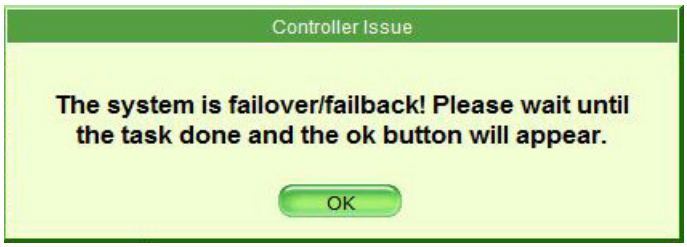


Figure 5-14 Controller failback message

If both controllers are down, the following pop-up dialog box will be displayed to notify the user.

Figure 5-15 Error message indicates both controller failures

5.4 Snapshot

5.4.1 Introduction

Snapshot allows you to create instantaneous data images of a volume at designated points in time. Unlike traditional data copy, which takes hours or even days for data replication, depending on the size of the volume, the snapshot function can create a copy of a volume of any size within seconds. In addition, creating a snapshot volume requires only partial capacity of the original volume, so snapshot is indeed a convenient solution in terms of time and capacity efficiency.

Because the snapshot is done at the array and block level by leveraging the computing power of the RAID controller, it is host-independent, and application-independent. It also causes less performance impact comparing to host-based snapshot software solutions.You are also allowed to restore data of a LUN using snapshot restore function. As the data image can be rolled back to a snapshot immediately, you may resume your applications without waiting time.

Below are a few examples of using the snapshot function:

- **Disk-based Full-image Backup and Restore**

  With snapshots of a volume at different points in time, you can retrieve files of old revisions or restore deleted files simply by mounting the LUN of the snapshot volumes. Contrary to tape-based backup, backup and data restoration is simpler and faster.

- **Reducing Data-freezing Time for Backup or Replication**

  When doing backup or data replication, the data of a volume has to be frozen to maintain the data consistency by pausing the I/O access of the applications. With the snapshot function, a copy of a volume can be created instantaneously, and the backup or replication operations can be performed on the snapshot volume, so the time to freeze a volume for backup can be largely reduced.

- **Testing Applications with Real-World Data**

  Because snapshot is created from production volume and its data is writeable independently from the original volume, you can use the snapshot to test new applications to find potential problems after software upgrade or patch.

- **Supporting SAN-based Applications**

  A snapshot volume can be exported to other host computers to offload the backup or other applications from the host computers owning the

working volume. This improves the system performance as well as frees you from installing all applications on all the host computers.

NOTE

Please test your backup scenarios and restored data with your applications. For sophisticated applications, like database, the restored data of the primary volume has to be in sync with data on other volumes in order to ensure proper operations of the applications.

5.4.2 How Snapshot Works

- **Snapshot Volume Pair and Copy-On-Write Operations**

  Before creating snapshots for a working volume, another volume (secondary volume) is needed to be associated with the working volume (primary volume) to form a snapshot volume pair. You can use JBOD disks, logical disks, or volumes as primary or secondary volumes. After a snapshot is created, the write commands to the primary volume will invoke "copy-on- write" (COW) operation, which copies the old data from the primary volume to the secondary volume before updating the primary volume with the new data. The COW operation preserves the data, and the primary volume can still be accessed.

- **Secondary Volume and Lookup Table**

  A snapshot volume is a virtualized entity, which leverages the data and space both on the primary and secondary volume. When an I/O command reads the snapshot volume, it retrieves the data either from the primary volume if the data is not updated or from the secondary volume if the data has been changed. And writes to a snapshot volume will be also stored in the secondary volume. A lookup table is maintained in the secondary volume for the RAID controller to know where the differential data is stored. Because the secondary volume stores only the differential data, you can choose a secondary volume of capacity less than the primary volume. However, to ensure minimum operations, the capacity of the secondary volume has to be at least 10 percent of the primary volume. A user-configurable overflow alert can notify you when the secondary volume has been filled up with the differential data over capacity threshold.

- **Spare COW Volume**

  When running out of the space of a secondary volume and there are spare COW volumes, the copied data of COW operations will be automatically redirected to an unused spare COW volume for the primary volume. The spare COW volume serves as a buffer to accommodate written data of size larger than planned and allows you to expand size of the secondary volume later. Although a spare COW volume can be used by any primary volume, one spare COW volume can be used by one primary volume at a time. For example, if you have

one spare COW volume and you have two primary volumes with overflow problems, then you can keep only the snapshots of the first primary volume that acquires the spare COW volume. As a result, it is advised to create multiple spare COW volumes if you have multiple primary volumes.

- **Multiple Concurrent Snapshots**

  A primary volume can have multiple snapshots at the same time. The old data of snapshots at different points in time shares single secondary volume and spare COW volume. **Figure 5-15** shows the relationship of primary volume, secondary volume, and snapshot volumes. However, when there are snapshot volumes, the COW operation would cause performance impact to the primary volume, and access to the snapshot volume would take longer time because of data lookup overhead in the secondary volume. You will experience more performance degradation when more snapshot volumes are being accessed at the same time.

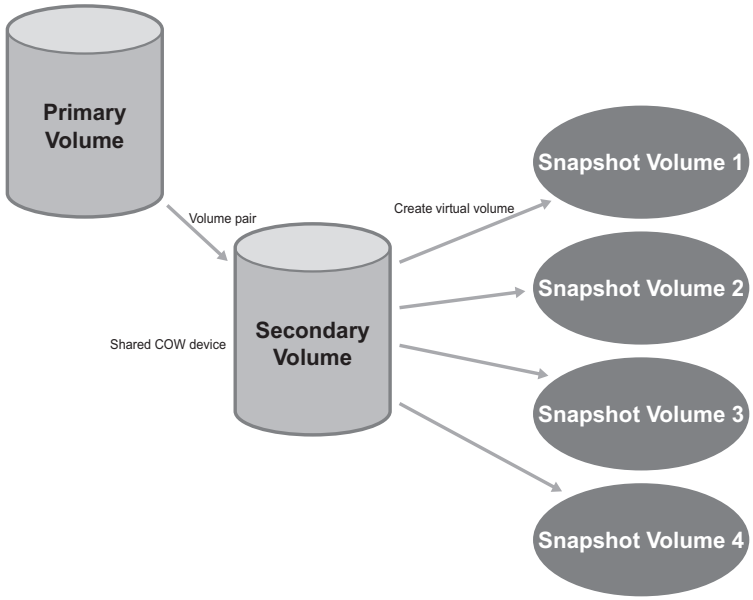


Figure 5-16 Relationship of volumes

- **Restoring by Snapshots**

  Users can online restore a primary volume to one of its snapshot volumes. After the restore, the contents of the primary volume immediately become the current image of data of the selected snapshot volume, and the primary volume is accessible. A backward synchronization task is started in the background to copy data of segments from the secondary volume and spare COW volume to overwrite the differential data on the primary volume. During the restoring, the I/O access to the primary volume and the other snapshot volumes can still be processed normally, but only after the restoring is done, new snapshots can be created again.

- **Online Volume Expansion**

The capacity of primary volume, secondary volume, and spare COW volume can be expanded without interfering with the operations of the snapshot volumes. After the capacity expansion operation is done for a volume or a logical disk, the new capacity can be automatically recognized and utilized by the snapshot functions. You may use this feature to allocate limited space for secondary volume and expand the secondary volumes later when more hard disks are available.

NOTE

1. The total maximum number of volume pairs is 64/16 for 512MB/ 1GB (1GB/512MB) memory installed.
2. The total maximum number of snapshot volumes is 512
3. The maximum number of snapshot volumes per primary volume is 32
4. The maximum capacity of primary/secondary/spare COW volume is 16TB
5. The minimum capacity of secondary volume is 32MB
6. The minimum capacity of spare COW volume is 128MB
7. The maximum number of spare COW volumes is 128

5.4.3 How to Use Snapshots

- **Overview**

To make the most use of the snapshot function, proper planning and configuration is of essence. Below is a list of related tasks grouped into three phases:

Phase 1: Planning

1. Identify the source volumes that need to have snapshots.
2. Define how many snapshots will be taken and how long they will exist.
3. Allocate the disk space and RAID attributes of the secondary volumes.
4. Allocate the disk space and RAID attributes of the spare COW volume.

Phase 2: Configuration

5. Create volumes of the secondary volumes.
6. Select a secondary volume for each source volume (primary volume).
7. Set up snapshot options, like overflow alert.
8. Build snapshot automation scripts and conduct trail runs (optionally).

Phase 3: Creating and Utilizing Snapshots (Manually or Scripted)

When taking a snapshot for a source volume, the tasks below are required:

9. Stop all the write access to the LUN of the primary volume.
10. Flush the cached data on the memory of your host systems.
11. Create the snapshot volume.
12. Resume the write access to the LUN of the primary volume.
13. Export the snapshot volume to a LUN for your applications (optionally)
14. Copy the data from the snapshot volume to other places (optionally)
15. Delete the snapshot volumes (optionally) to avoid running out of space on the secondary volumes.

The tasks in the phase 1 and 2 are done only once when you set up a RAID system or when you create a new LUN. They could also be parts of your RAID system reconfigurations. The tasks in phase 3 are very likely to be repeated periodically when a snapshot is needed.

- **Planning for the Secondary Volumes**

When planning your storage resources, you have to reserve sufficient free capacity for the secondary volumes. In addition to the space reserved for the RAID controller to build lookup tables, the capacity reserved for the secondary volumes depends on how much data could be modified on the primary and snapshot volumes during the life time of the snapshot volumes. If you keep the snapshot volumes longer, it is more likely that more data will be modified. A commonly-used capacity of a secondary volume is 20% of the source volume.

However, not all write commands would consume space of the secondary volume. For single block on the primary and snapshot volume, the copy operation and space allocation on the secondary volume is performed only at the very first time when a write command hits the block. As a result, if write commands tend to hit the same blocks, you may consider using a smaller secondary volume.

Another consideration in estimate reserved capacity is that because the COW operations are done by chunks, consisting of multiple consecutive sectors, more space is required than the actual data being modified.

If the space of a secondary volume is fully occupied, the data on the snapshot volumes will be corrupted. Be aware of applications that would change huge amount of data on a source volume, like video recording and file system defragmentation. If all the data will be changed, ensure that the secondary volume's capacity is set to 105% of the size of the source volume.

You will also properly set the RAID attributes of the secondary volume depending on your performance and reliability requirements for the snapshot volumes. It is advised that the secondary volumes are located on the different disk group of the primary volumes, such that the COW operation and the I/O access to the snapshot volume can be done more efficiently.

NOTE

1. Set spare COW volumes to avoid data loss in the snapshot volumes when the space of the secondary volume is overflow.
2. Expand secondary volume or spare COW volume to accommodate more differential data

- **Creating Snapshots using GUI or CLI**

After secondary volumes are chosen for the volumes need to have snapshots, you may create snapshots by the Web GUI or CLI commands. Detailed information about GUI and CLI can be found in **2.6.6 Snapshot Volumes on page 2-34** and **4.2 Basic RAID Management on page 4-7**, respectively. On Windows, you may also use the host-side CLI utility, **acs_snap.exe**. After copying the executable file to the directory where you want to run the utility on your host system, you can use the utility to create, list, and delete snapshot volumes for a LUN. However, because it communicates with the RAID controller by the in-band interface, your primary volumes have to be exported to host computers to get commands from the **acs_snap.exe** utility.

- **Pausing I/O at Hosts and Applications**

Before creating a snapshot, all write data on the LUN of the primary volume have to be committed to the RAID storage and no data structure is in the inconsistent state. Otherwise, the RAID controller would capture a corrupted data image that prohibits your operating systems or applications from using it. For example, if a money-transfer transaction completes only reducing the source and leaves the destination intact, the snapshot taken at this moment cannot get a balanced total sum of the money in the database. However, there are also operating systems or applications that can successfully recover from the database with partially-done transactions by journaling algorithms.

In contrary to stopping the applications manually, you may use the utility offered by your applications to force the applications to enter "quiescent" state, in which there is no ongoing transaction and all completed transactions have been made effective permanently. In some systems, you may try to un-mount the LUN to force the operating systems to flush cached data and to avoid I/O access when the snapshot is taken.

- **Dealing with Identical Data Images at Hosts**

  Some operating systems and applications could get confused when seeing more than one identical volume at the same time. In Windows, if a volume is configured as a dynamic disk, its snapshot volume will get the same Disk ID, and the Windows Logical Disk Manager will malfunction when both volumes are present. To avoid this problem, it is advised to export the snapshot volumes to other host computers, like a backup server. However, the type of operating systems to access the snapshot volumes should be capable of recognizing the data created by the host computer of the source volumes.

- **Retaining Permanent Data of Snapshots**

  Because a snapshot volume serves I/O by accessing the corresponding primary volume and secondary volume, its reliability and performance also depends on the configurations of these two volumes. The snapshot volume will crash if either of the two volumes is damaged. To completely retain the data in the snapshot volume for data protection or to avoid performance degradation, it is advised to copy the data from a snapshot volume to another volume or another RAID system. Applications that need to keep the snapshot data for a long time, like doing data mining, compression, or archival, having an independent data image is more suitable.

NOTE

A snapshot volume would crash when any of its primary volume, secondary volume, or spare COW volume crashes. A primary volume would crash if either secondary volume or spare COW volume crashes while it is in the restoring state. In the cases above, please delete the volume pair.

- **Restoring Data with a Snapshot**

  To restore data of a primary volume from a selected snapshot volume, please follow the steps below:

  (1) Unmount the LUN of the primary volume at the host computers

  (2) Remove the LUN mappings of the primary volume

  (3) Remove the LUN mappings of the snapshot volume (optional)

  (4) Issue the snapshot restore command from GUI or CLI

  (5) Restore the LUN mappings for the primary volume

(6) Mount the LUN of the primary volume at the host computers

NOTE

1. 1.Restoring data with a snapshot volume destroys the data on the primary volume.
2. If selecting a snapshot volume with LUN accessed by host computer, flush the system cache before unmouting the LUN of the snapshot volume.

- **Deleting Snapshots**

It is advised to delete any snapshot volume once you do not need it. Deleting a snapshot volume frees the space it occupies in the secondary volume, and if there is no snapshot, the performance of the primary volume will be back to normal. You can do it freely as long as no host is accessing it, and deleting one snapshot does not interfere with the other snapshots of the same source volume.

- **Snapshot Roaming**

The snapshot configurations are stored in the disks of the secondary volume. If **"Auto Array Roaming Control"** option is enabled please see **2.7.16 Miscellaneous on page 2-55**, foreign hard disks with snapshot configurations can be automatically restored during the controller boo-up. However, if **"Auto Array Roaming Control"** option is turned off or auto array roaming does not work due to configuration conflict, configurations of disk groups and logical disks have to be restored first by importing the foreign hard disks, and then you may proceed to manually import the snapshots by GUI or CLI please see **2.7.12 Array roaming on page 2-51**.After the snapshots are imported either automatically or manually, you need to set their LUN mappings.

NOTE

Abnormal shutdown of the RAID system could cause data loss of the snapshot volume if the lookup table on the secondary volume is not updated.

5.4.4 Snapshot Utility and Scripting

- **Using Snapshot Host-side Utility on Windows**

In addition to managing snapshot volumes, you may also use the snapshot utility, **acs_snap-win32-Vx.xx.exe,** to do cache flush. Its complete usage syntax is described as below:

Usage:

acs_snap create <device> <snapshot_name> |delete <device>

<snapshot_name> | flush <device> | list <device>

Examples:

1. Create a snapshot: **acs_snap-win32-Vx.xx.exe** create F: f_snap1_2pm

2. Delete a snapshot: **acs_snap-win32-Vx.xx.exe** delete PhysicalDrive2 db_2pm

3. Flush cache: **acs_snap-win32-Vx.xx.exe** flush F:

4. List snapshot information: **acs_snap-win32-Vx.xx.exe** list F:

The <device> denotes the name of drive **acs_snap-win32-Vx.xx** to carry on the command. It could be either logical drive letter (C: D: F:) or **PhysicalDrivex** where **x** is the number of the physical drive given by Windows.

When creating a snapshot, its name, <snapshot_name>, cannot be repeated within the same source volume, because <snapshot_name> is used as the identifier of the snapshot.

- **Scripting Snapshot Operations**

To illustrate using script in a SAN-based backup application, consider the SAN environment in Figure 5-24:

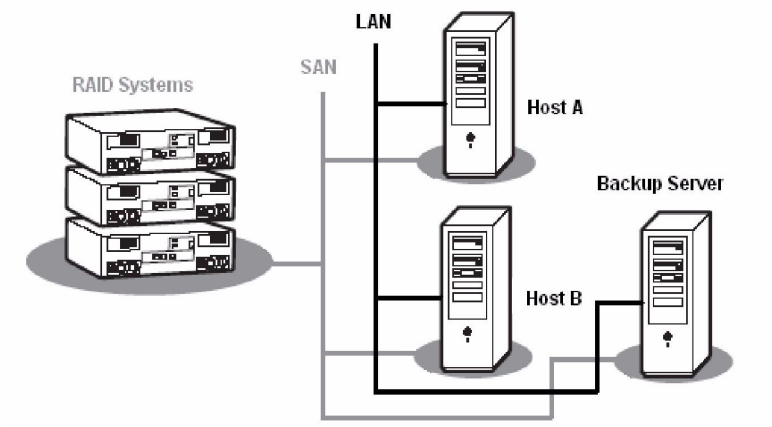


Figure 5-17 SAN Environment

The script below is to be executed by the backup server and it backs up the SQL server on the remote Windows 2003 hosts.

1.Net stop mssqlserver

2.rcmd \\192.168.0.1 C:\snapshot\acs_snap flush D:

3.rcmd \\192.168.0.1 C:\snapshot\acs_snap create D: sql_shot

4.Net start mssqlserver

5.RAID CLI to export the snapshot LUN to the backup server

6.Mount the snapshot LUN on the backup server (use mountvol)

7.Backup Software CLI to run the backup operations

8.rcmd \\192.168.0.1 C:\snapshot\acs_snap delete D: sql_shot

- ## Automating Snapshot Operations

  With this utility together with the instructions to stop and restart your applications, you may put them into a script file, and use the scheduling utility offered by the operating system to create snapshot at designated points in time or periodically. For example, in Windows, you click on **Start > Programs > Accessories > System Tools > Scheduled Tasks** to launch Schedule Task Wizard. Integrating the script with the snapshot applications, like backup or replication software, your tasks can be done more easily.

5.5 Dynamic Capacity Management

The RAID controller enables flexibility in capacity configuration and reconfigurations for the following benefits:

- Improving the utilization of disk capacity
- Lowering the cost of hard disks in term of procurement and energy
- Easy management without down time

• Comprehensive capacity management utilities

The firmware utilities below allow you to increase disk space:

- Delete unused logical disks to release free space (Section **2.6.4 Logical disks**)
- Delete unused volumes to release free logical disks (Section **2.6.5 Volumes**)
- Expand a disk group by adding hard disks to it (Section **2.7.1 Expanding disk groups**)
- Shrink under-utilized logical disks to release free space (Section **2.7.5 Shrinking logical disks**)
- Shrink under-utilized volumes to release free logical disks (Section **2.7.7 Shrinking volumes**)

The firmware utilities below allow you to manage or utilize free disk space:

- Create logical disks using free space on a disk group (Section **2.6.4 Logical disks**)
- Create volumes using one or more free logical disks (Section **2.6.5 Volumes**)
- Defragment a disk group to merge free chunks into one (Section **2.7.2 Defragmenting disk groups**)
- Expand over-utilized logical disks with free chunks (Section **2.7.4 Expanding the capacity of logical disks in a disk group**)
- Expand over-utilized volumes with free logical disks (Section **2.7.6 Expanding volumes**)

• LUN resizing (capacity expansion/shrink) procedures

The resizing of a logical disk or volume changes the usable capacity of a LUN. The LUN capacity change is made effective after the background task is done for logical disk expansion, and it is effective immediately after your UI operation for other resizing utilities (expanding volumes and shrinking volumes/logical disks).

To ensure your host can properly recognize and utilize the expanded space, please follow the steps below in order:

(1) Expand a logical disk or a volume by the firmware utility

(2) Wait till the background task is done (for logical disk expansion only)

(3) Rescan the physical drives by your operating system utility

(4) Expand the partition on the LUN by your partition editor

(5) Expand the file system on the expanded partition by your file system utility

To ensure your host can properly recognize and shrink the corresponding space without data loss, please follow the steps below in order:

(1) Ensure enough unused space in the file system of a partition

(2) Shrink the file system on the partition by your file system utility

(3) Shrink the partition on the LUN by your partition editor

(4) Shrink the corresponding logical disk or volume by the firmware utility

(5) Rescan the physical drives by your operating system utility

- **Capabilities at host to support LUN resizing**

Proper LUN resizing depends on the capabilities of your operating system, partition editor, and file system utilities. It is advised to check the related manuals and do some trial runs before doing LUN resizing for your production site. You may use file system check utilities after the resizing for ensuring data integrity.

Below list the software that offers solutions to support partition resizing:

- Symantec Partition Magic : **http://www.symantec.com/**
- Paragon Partition Manager: **http://www.paragon-software.com/**
- Arconis Disk Director: **http://www.acronis.com/**
- Coriolis Systems iPartition (MAC OS): **http://www.coriolis-systems.com/**

There are also utilities offered by operating systems or file systems, and below are some examples:

- Windows 2003 server or later: DiskPart, see **5.5.6 Windows DiskPart Utility**
- Linux ext2/ext3 file systems: resize2fs
- Linux ReiserFS file system: resize_reiserfs
- Linux XFS file system: xfs_growfs
- Linux GNU parted partition editor: **http://www.gnu.org/software/parted/**
- Symantec Veritas VxFS: fsadm and extendfs

Below are some commonly-seen restrictions regarding to file system and partition resizing:

- A LUN for resizing can have only one primary partition and no extended partition.
- A boot partition with operating system on it might not be shrunk
- Rebooting the OS might be needed after the resizing
- Resizing partition or file system might have to be done offline
- File system defragmentation might be needed before resizing

NOTE

The software listed above is only for your information; no warranty should be assumed. Please contact the software vendors to learn how to use the software to support LUN resizing.

- **Comparisons with thin provisioning**

Dynamic LUN resizing is better than thin provisioning in terms of reliability and performance because it retains the linear and contiguous data layout:

- Thin provisioning needs to maintain address translation tables, which could cause disastrous data loss when corrupted.
- The over-advertised capacity of thin provisioning misleads the space allocation algorithm of a file system.
- The scrambled data layout of thin provisioning cause bad performance, especially when sharing storage of different types of workloads or host computers.
- Thin provisioning is very likely to be misled to allocate unnecessary space by data movement or data scrubbing applications, like file system defragmentation.

5.5.1 Free chunk defragmentation

The free space on a disk group is managed as free chunks. When there is no logical disk on a disk group, all the available space forms a free chunk. Later, free chunks are created when you delete logical disks or shrink the capacity of logical disks, but adjacent free chunks will be merged automatically. You can use free chunks for creating new logical disks or expanding a logical disk.

A logical disk has to use contiguous space on a disk group, so you need to merge all free chunks into one by the disk group defragmentation utility, which starts a background task to move the data of all logical disks on the disk group to the beginning space of the hard disks, such that all free space is consolidated to form single free chunk located at the ending space of the hard disks. Two common scenarios are illustrated as below:

- **Disk group expansion to expand the last existing free chunk**

All existing free chunks except the one at the end of the disk group are deleted, and the last free chunk is expanded.

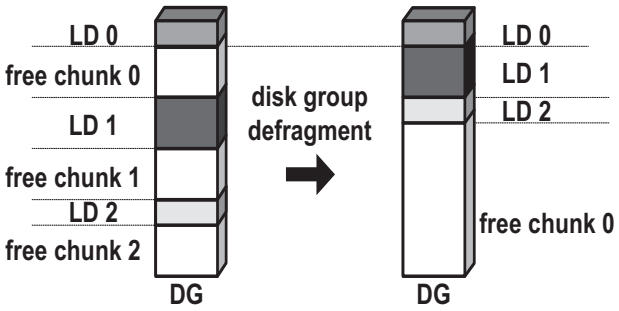


Figure 5-18 Defragment a disk group to expand the last free chunk

- **Defragment a disk group to consolidate free chunks**

All existing free chunks are deleted, and a single free chunk at the end of the disk group is created.

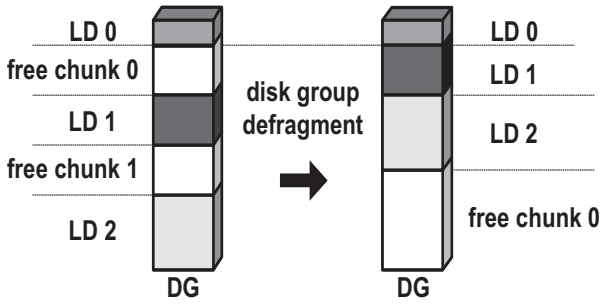


Figure 5-19 Defragment a disk group to consolidate free chunks

5.5.2 Logical disk shrink

Logical disk shrink can be used to decrease the capacity of a logical disk. When performing logical disk shrink, the capacity of the corresponding LUNs will be modified immediately and any attempt to access to the space beyond the new capacity will be rejected. You have to shrink the partition and the file system on the host computer before shrinking the logical disks in order to avoid data loss.

- **Shrink logical disk with an adjacent free chunk**

When a logical disk is shrunk, the free chunk right after the logical disk is expanded by the capacity reduced at the shrunk logical disk.

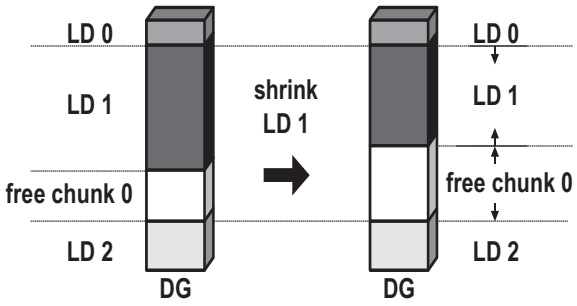


Figure 5-20 Logical disk capacity shrink and expanding an adjacent free chunk

- Shrink a logical disk without an adjacent free chunk

  After a logical disk is shrunk, a free chunk is created next to the logical disk.

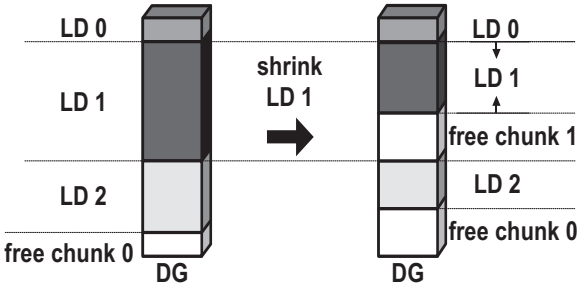


Figure 5-21 Logical disk capacity shrink and creating a new free chunk

5.5.3 Logical disk expansion

Logical disk expansion can be used to increase the capacity of a logical disk by allocating free chunks and by moving logical disks in the same disk group to consolidate a free chunk for the new space of the selected logical disks.

- Expand a logical disk by allocating an adjacent free chunk

  If there is a free chunk right after the logical disk, the required capacity of the logical disk can be allocated immediately via the free chunk.

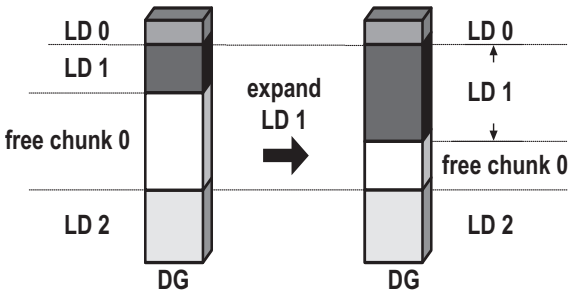


Figure 5-22 Logical disk capacity expansion by allocating an adjacent free chunk

- Expand a logical disk by moving logical disks to a free chunk

If there is no free chunk right after the selected logical disk, the controller will start a background task to move nearby logical disks to fill the requested capacity.

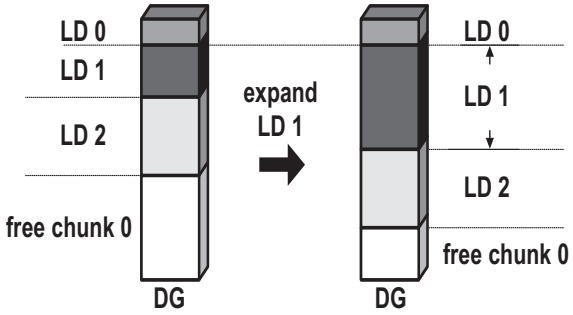


Figure 5-23 Logical disk capacity expansion by moving logical disks to a free chunk

- **Expand a logical disk by allocating an adjacent free chunk and moving logical disks**

If the free chunk right after the selected logical disk is not sufficient for expansion, the controller will allocate the free chunk and also start a background task to move logical disks.

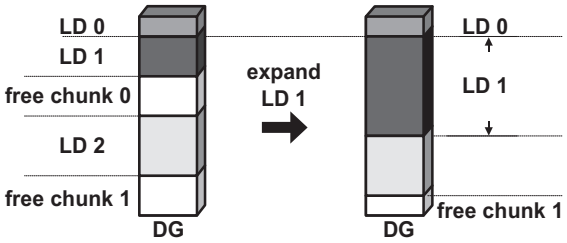


Figure 5-24 Logical disk capacity expansion by allocating an adjacent free chunk and moving logical disks

5.5.4 Disk group expansion

Disk group expansion can be used to increase the useable space of a disk group by adding one or more disks to the disk group. When the expansion task is complete, the new space is created in the end space of the disk group. Logical disks can be created in the space set up by the expansion.

- **Disk group expansion to expand the last existing free chunk**

If the disk group has free chunks in the end space, the capacity of the free chunk will be increased after the expansion. The capacity of existing logical disks will not be affected.

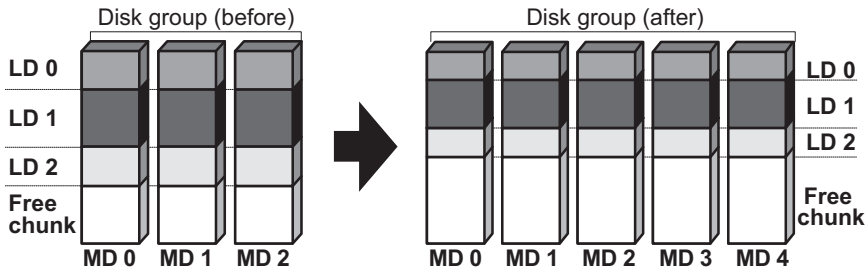


Figure 5-25 Disk group expansion by adding new member disks and enlarging the last free

- Disk group expansion to create a free chunk

If the disk group has no free chunks in the end space before expansion, a new free chunk will be created.

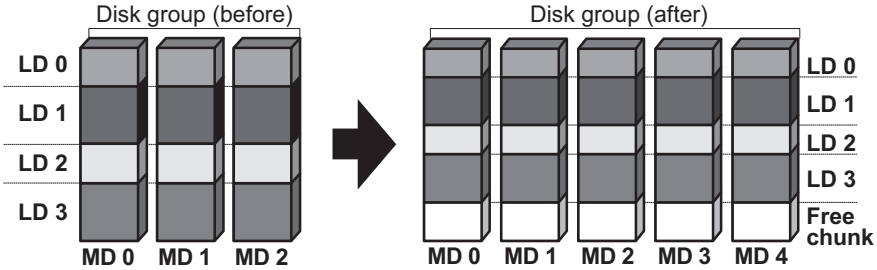


Figure 5-26 Disk group expansion by adding new member disks and creating a new free chunk

- Disk group expansion to consolidate free chunks

When disk group expansion is executed in a disk group where free chunks between logical disks exist, the free chunks are consolidated and placed in the end space of the disk group after expansion.

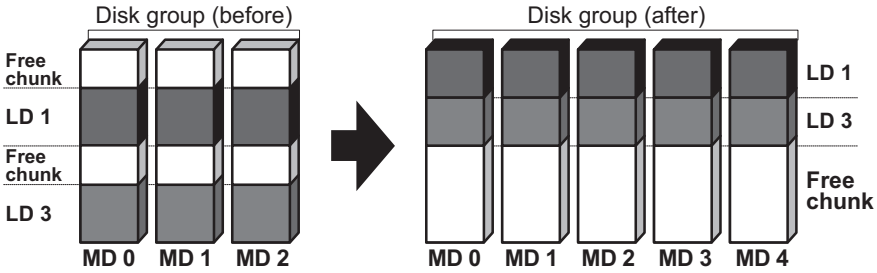


Figure 5-27 Disk group expansion to consolidate free

NOTE

It is suggested that defragmentation should be performed during disk group expansion. In the cases shown in Figures 5-24, 5-25, and 5-26, defragmentation forms an organized collocation for all logical disks and free chunks after expansion.

5.5.5 Volume expansion and shrink

The capacity of a volume can be online expanded by adding the logical disks to the volume, which concatenates the space of each logical disk to form a larger capacity. Because the expansion is done instantly without incurring any background tasks, you can quickly start using the added capacity without waiting. Users can also reduce the capacity of a volume by removing the concatenated logical disks. Freely expanding and shrinking a volume enables efficient storage resource management.

Striping: A volume formed by single volume unit.

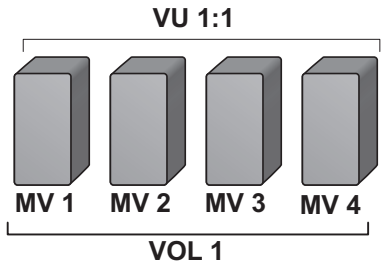


Figure 5-28 Striping member

Concatenating: A volume formed by multiple volume units.

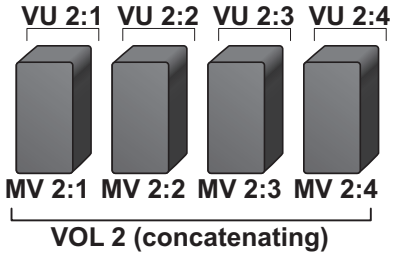


Figure 5-29 Concatenating member

Concatenated striping: A volume formed by concatenating set of striping member volumes.

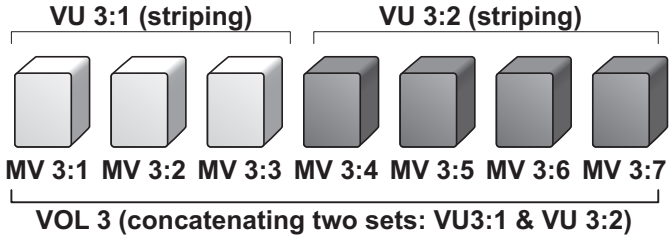


Figure 5-30 Concatenated striping member

5.5.6 Windows DiskPart Utility

The Microsoft Diskpart utility is a command line program for managing the disk partitions or volumes on Windows systems. You can use it for repartitioning drives, deleting partitions, creating partitions, changing drive letters, and shrinking or expanding volumes by using scripts or direct input from a command prompt. The Diskpart utility is embedded in Windows Server XP, 2003, and Vista operating system. It can also support Windows 2000, but you need to download it from Microsoft web site.

For a list of commands that you can use within the Diskpart console you can type **help** to get some information. For the help instructions for a particular command you can type the name of the command followed by help, such as **select help**.

The Diskpart utility can support online expansion of basic and dynamic disks for all Windows operating systems, but partition shrinking is supported only on Windows Vista. Below are basic examples to illustrate how to do expansion and shrink by the Diskpart.

NOTE

For details about the capabilities and limitations of the Diskpart utility, please check Microsoft web site, and make sure you have a full backup before the operations.

- **Do extend a partition:**

Before expansion, please make sure that there is contiguous free space available next to the partition to be extended on the same LUN (with no partitions in between). If there is no free space, you can extend the LUN by extending its corresponded logical disk or volume in the RAID system.

Step1: At a command prompt, type: Diskpart.exe (Launches the utility.)

Step2: At the DISKPART prompt, type: Select Disk 1 (Selects the disk.)

Step3: At the DISKPART prompt, type: Select Volume 1 (Selects the volume.)

Step4: At the DISKPART prompt, type: Extend Size=5000 (If you do not set a size, such as the above example for 5 GB, it will use all the available space on the current disk to extend the volume.)

When the extend command is done, you should receive a message stating that Diskpart had successfully extended the volume. The new space should be added to the existing logical drive while maintaining the data.

- **Do shrink a partition:**

Shrinking a partition can release free space for other partitions on the same LUN. Or, after the partition shrinking is done, you may shrink the LUN to release free space for other LUNs.

Step1: At a command prompt, type: Diskpart.exe (Launches the utility.)

Step2: At the DISKPART prompt, type: select disk 1 (Selects the disk.)

Step3: At the DISKPART prompt, type: select volume 1 (Selects the volume.)

Step4: At the DISKPART prompt, type: shrink desired=2000 (If you do not set a size, such as the above example for 2 GB, it will shrink the partition by the maximum amount possible. You may use shrink querymax command to know the maximum space that you can shrink.)

When the shrink command is done, you should receive a message stating that Diskpart had successfully shrunk the volume. The partition space should be subtractive to the existing drive while maintaining the data on the volume, and there will be unallocated space created.

NOTE

Rebooting the host computers might be needed so as to make it effective.

On Windows Vista, you can also use Computer Management ÑŠ Disk Management GUI to do partition expansion and shrinking.

Please follow the links below and enter "diskpart" to find more information:

Microsoft Web Site Links:

Search link:

http://search.microsoft.com/?mkt=en-US

Download diskpart utility link:

http://www.microsoft.com/downloads/details.aspx?FamilyID=0fd9788a-5d64-4f57-949f-ef62de7ab1ae&displaylang=en

5.6 RAIDGuard Central

5.6.1 Introduction

RAIDGuard Central is a software utility that allows you to remotely monitor multiple RAID systems located at different networks, and to consolidate event logs from these RAID systems at a single console. It also offers smart discovery of RAID systems and real-time event notification by MSN messages. The features and benefits of RAIDGuard Central are summarized as below:

- Remote monitoring multiple RAID systems

With RAIDGuard Central, you can watch the status of multiple RAID systems by single GUI console, which can be launched either locally or remotely by a web browser. You can quickly know the status of all RAID systems simply at one glance, and when there is an event happening to a RAID system, you can launch the web GUI of the RAID system by RAIDGuard Central to know further details of the RAID system or conduct maintenance tasks. This helps you quickly locate the RAID systems in trouble and frees you from checking the GUI of each RAID system.

- Consolidating event logs of multiple RAID systems

RAIDGuard Central keeps monitoring the RAID systems and stores the event log from the RAID systems to local files. You can browse the event logs of the RAID systems registered in RAIDGuard Central to know the complete event history or to export the event log to files. Because the old event logs stored on the controller will eventually be overwritten by latest events due to limited space of NVRAM, using RAIDGuard Central can help to keep as many event logs as you need.

- Support multiple network segments

When RAID systems are located at different network segments, RAIDGuard Central can still monitor these RAID systems and collect their event logs by introducing one RAIDGuard Central Agent for each network segment. RAIDGuard Central Agent bridges between the RAID systems in the same local network and RAIDGuard Central, and performs RAID system discovery and monitoring on behalf of RAIDGuard Central.

- Enable access to web GUI of RAID systems in private networks

RAIDGuard Central and its agents forward the transactions of web GUI access between a web browser and the RAID systems located in a private network. You can use the web GUI for RAID system remote monitoring and full-function management of a RAID system even if the local network of the RAID system uses virtual IP addresses.

- Instant event notification by MSN messages

IM (Instant Messaging) services have become an important part of communication because of its ease-of-use and timeliness. RAIDGuard Central leverages the most popular IM service, Microsoft MSN, to deliver

event information of RAID systems to specified MSN accounts. This ensures that you get timely updates on the status of your RAID system.

- Smart discovery of RAID systems

RAIDGuard Central is the portal of your RAID system management. Instead of remembering the IP address of each RAID system, you can use RAIDGuard Central to scan the networks to discover the RAID systems attached to the networks. After RAIDGuard Central locates the RAID systems, you may access the web GUI of the RAID systems.

- Support multiple platforms

Based on Java and web technologies, RAIDGuard Central Server and its agents support the most popular operating systems: Windows, Linux, and Mac. You may choose the most appropriate platforms to perform the RAID monitoring and event consolidation tasks according to the environments. In addition, RAIDGuard Central provides web-based GUI, which also enables you to check the status of RAID systems from any places where Internet connection is available.

- Support multiple languages

RAIDGuard Central currently supports three languages: English, Traditional Chinese, and Simplified Chinese. The default language will be automatically selected according to the default locale of the computers running RAIDGuard Central, and you may also set the language manually. RAIDGuard Central allows adding more languages. Please contact your RAID system supplier if you want to use other languages.

5.6.2 Deployment Overview

RAIDGuard Central consists of the following three software components: RAIDGuard Central Server (RGC Server), RAIDGuard Central Agent (RGC Agent), and RAIDGuard Central GUI (RGC GUI). RGC Server is the main software component of RAIDGuard Central, responsible for RAID system monitoring, event consolidation, and event notification. RGC Server communicates with RGC Agents, which are installed on computers in different networks (one RGC Agent for one network), to discover RAID systems and receive events. RGC Server also provides information to the RGC GUI, which may be launched either locally on the same computer of RGC Server or remotely with web browsers (RGC Server is embedded with a web server). When you launch the web GUI of a RAID system on RGC GUI, the RGC Server and RGC Agent will forward the packets between the remote web browser and the web GUI server on the RAID system.

The illustration below shows how RGC software components can be deployed to build a centralized RAID management and monitoring infrastructure. A computer is chosen to execute RGC Server, and RGC Agents are installed to different networks for communicating with the RAID systems in each network. Note that RGC Server alone cannot communicate with RAID systems, you need to install also an RGC Agent

to a computer (may be the same as the one of RGC Server) in the same network of RGC Server, if there are RAID systems in that network.

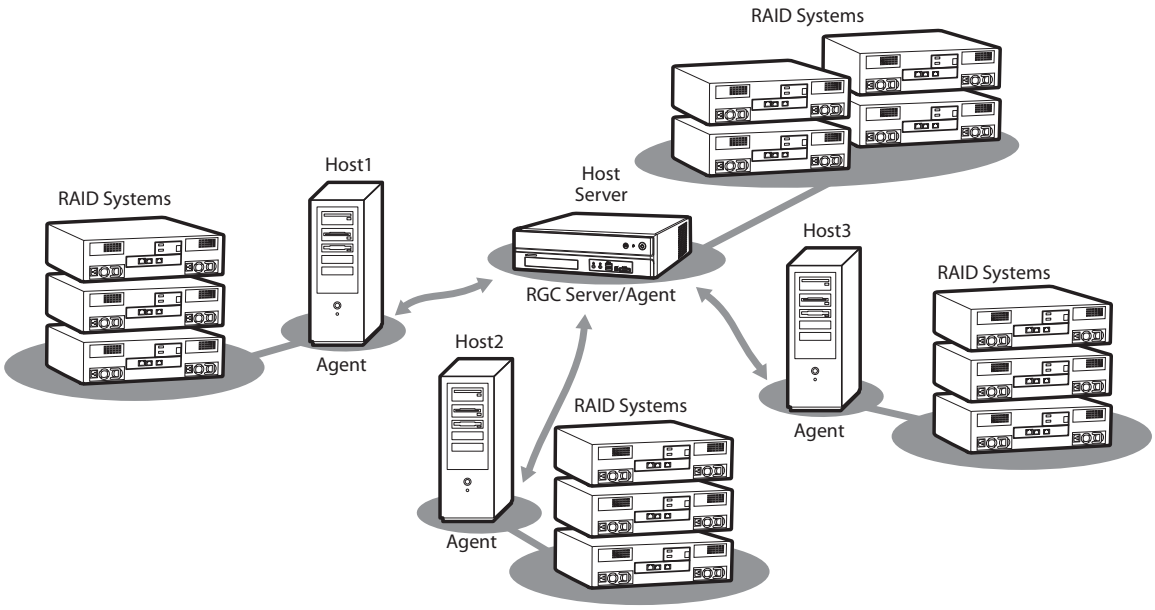


Figure 5-31 Deployment example of RAIDGuard Central components

You may follow the steps below to deploy the RGC components:

1. Install RAID systems and connect them to the networks.
2. Install one RGC Server and conduct the necessary configurations (you need to start web server if you would like to use RGC GUI).
3. Install RGC Agents (one for each network segment).
4. Launch RGC GUI (you will need to enter a password).
5. Use RGC GUI to add RGC Agents by keying the IP address of the RGC Agents.
6. Use RGC GUI to discover the RAID systems for each RGC Agent.
7. Use RGC GUI to register the discovered RAID systems (you need to present the administrator's password of the RAID systems for registration).
8. Configure MSN accounts for event notification (optional).

Now you may freely read the status and events of all registered RAID systems by RGC GUI.

When there are new RAID systems installed to a network with an RGC Agent, you need to use RGC to rescan the network to discover and register the new RAID systems. When there are new RGC Agents, you will need to add these RGC Agents to your RGC Server by RGC GUI.

If RAID systems are attached to a private network with virtual IP address, the computer running RGC Agent for this network must have a real IP address such that RGC Server can communicate with the RGC Agent.

This can be done by creating a mapping in the gateway of the network and assign a real IP address to the computer.

Note that when there is constant heavy network traffic, the communication between RGC components would be influenced and the operations would become slow. When the network connection between RGC Server and RGC Agents is down, the status and the latest events of the RAID systems managed by the RGC Agents will not be visible. But after the network connection is recovered, the RGC Server will synchronize its local event database with the event logs on the RAID systems. For easing the management, you may also consider dividing the RAID systems into two or more domains, and install one RGC Server for each domain. But note that one RGC Agent can be accessed by only one RGC Server.

To avoid discontinued monitoring because of the failure at the monitoring sites, you may set up two RGC Servers to monitor the same set of RAID systems. The monitoring tasks can still continue when one of the RGC Servers is down.

NOTE

1. The RGC components communicate with each other by the TCP connections at the following ports: 8060~8070, 8077, and 8088. Make sure the network connection and these ports are not blocked by your firewall equipments and software before deploying RGC components. Please also make sure these TCP ports are not used by other applications running on the computer of RGC Server and Agents.
2. Running RGC components requires Java Runtime Environment (JRE) version 1.5 or later on the computers.

5.6.3 Installing the RAIDGuard Central

The RAIDGuard Central provides software installation files for all supported operating systems. You can choose the installation file and follow the setup procedures below depending on the operating system you are using.

1. Copy the installation file to the host computer on which you want to install the RAIDGuard Central.
   - Windows OS installation file: setup.exe
   - MAC OS installation file: RAIDGuardCentral_SW_x.xx.mpkg
   - Linux OS installation script: RAIDGuardCentral_SW_x.xx.run
2. Double click the installation file to start the installation.
3. Follow the on-screen instructions to complete the installation.

NOTE

The RAIDGuard Central provides three installation options: complete RGC components, RGC server only, and RGC Agent only.

5.6.4 Uninstalling the RAIDGuard Central

Follow the steps below to uninstall the RAIDGuard Central from the host server.

- **Windows OS platform**

1. Click **Start > Settings > Control Panel > Add or Remove Programs**. Locate **RAIDGuard Central** and click **Remove** to begin uninstallation.
2. An uninstallation message pops up. Click **Yes** to continue or **No** to abort.
3. The uninstaller starts to remove the RAIDGuard Central from your computer.

- **Mac/ Linux OS platform**

To uninstall the RAIDGuard Central from your Mac or Linux operating system, simply delete the folder where the RAIDGuard Central program files are located.

5.6.5 Launching the RAIDGuard Central

When the installation is finished, launch the RGC Server and RGC Agent monitor screens as described below:

In Windows OS: Go to **Start > Programs > RAIDGuard Central > RAIDGuard Central** or **RAIDGuard Agent**.

In Mac OS: Go to **Application > RAIDGuard Central > RGC.jar or RGCAgent.jar**.

In Linux OS: You can use either of the following ways to launch the RGC Server and RGC Agent.

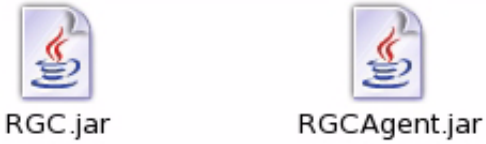
- Run the Linux terminal and type in the following commands to execute the RGC Server and RGC Agent:

  ./java installation directory/java -jar RGC.jar or

  ./java installation directory/java -jar RGCAgent.jar

  By default, the java application is installed in "/usr/java/jdk1.6.0_01/bin". The default installation directory depends on the JRE version and the operating system in use.

- Double click the .jar executable file (RGC.jar or RGCAgent.jar) in the folder it belongs to. Ensure that the application connection has been set so that you can open the file. For more information on setting up the connection between the .jar executable file and the java application, see the instructions provided by your Linux operating system.



NOTE

If you want the RAIDGuard Central loading at startup each time the host computer is turned on, refer to your operating system documentation to find out how to add the startup programs.

- **RGC Server and RGC Agent Monitor Screens**

The RGC Server monitor screen (based on Windows platform) is displayed as below:

Figure 5-32 RGC Server monitor screen

The following table describes the function of each menu bar item, buttons, and listed information in this screen.

Menu Bar	
System	**Exit:** Exit the program.
Language	Specify the desired GUI language. * The language options will differ according to the language support on your operating system.
Help	**Help Contents:** Open the online help web page. **About:** Display the program version.
Buttons	
Start Server / Stop Server	Start or stop the web server at the specified port. * If the web server is stopped, the RGC GUI cannot be used, but RGC can still receive events generated from RAID systems.
Change Port	Change the new listening port. The web server listens for requests at port 8080 by default. The range is from 1 to 32767.
Launch RGC GUI	Launch the RGC GUI.

Listed Information	
Web Server Status	Display the current status of server: *Inactive* or *the current listening port*.
Web Server Port	Display the current server port.
Connecting Users	Display the number of users logged into the RGC GUI.

NOTE
RAIDGuard Central supports only login with the *admin* account.

The RGC Agent monitor screen (based on Windows platform) is displayed as below:

Figure 5-33 RGC Agent monitor screen

The following table describes the function of each menu bar item and listed information in this screen.

Menu Bar	
System	**Exit:** Exit the program.
Language	Specify the desired GUI language. * The language options will differ according to the language support on your operating system.
Help	**Help Contents:** Open the online help web page. **About:** Display the program version.
Listed Information	
Registered RGC	Display the RGC Server address the current agent belongs to. Otherwise 'None' is displayed.
Registered Systems	Display the number of RAID systems registered to the current agent.

NOTE
There is almost no limitation to the maximum number of RAID systems registered to RAIDGuard Central.

5.6.6 RGC GUI Overview

- **Login**

To launch RGC GUI, you may click the **Launch RGC GUI** button on the RGC Server monitor screen. You can also access the GUI remotely with a web browser by entering the URL: http://RGC-IP:xxxx/RGCG, where *RGC-IP* is the IP address of the computer running RGC Server, and xxxx is the port of the RGC web server is listening to.

NOTE

1. The RGC GUI is a java-based software utility. Each time you open the RGC GUI, a java webpage displays, which is used to run the java applet. Then a warning message pops up for digital signature verification. Click **Run** to enter the login screen.
2. Please always keep the webpage used to run the java applet open or minimized in the task bar so that you can view and use the RGC GUI properly.

After logging into the RGC GUI, the following screen displays:

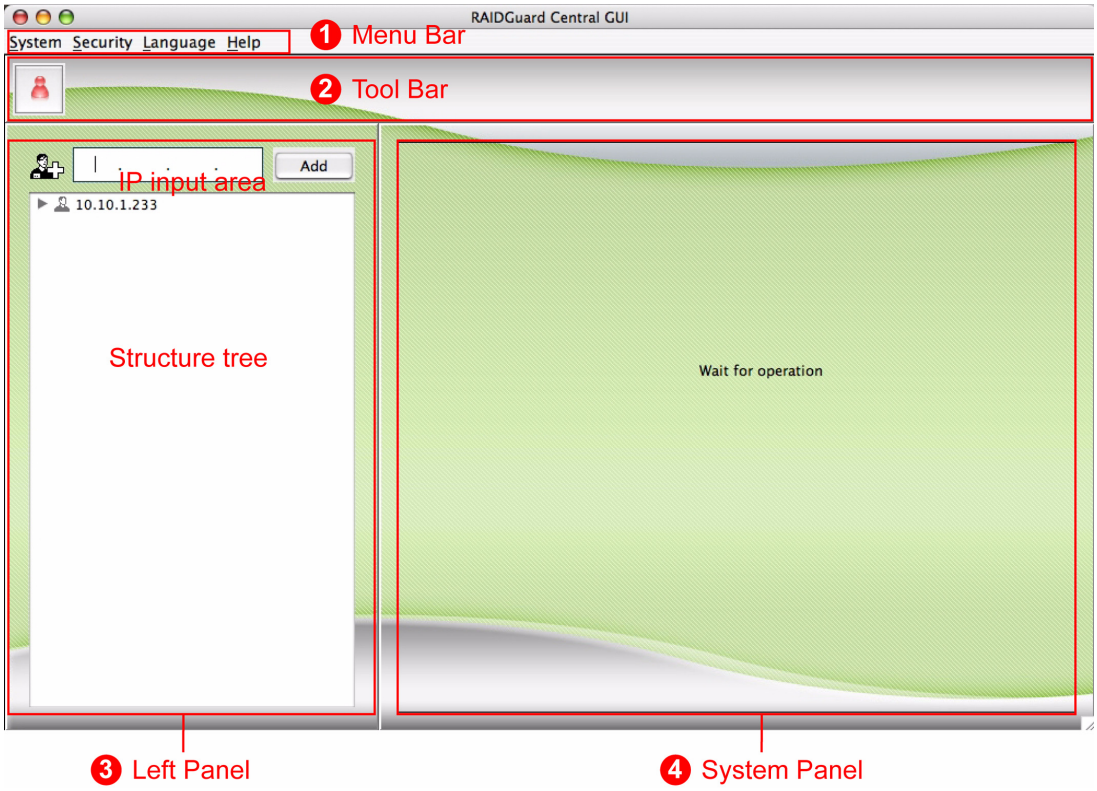


Figure 5-34 RGC GUI main screen

The following table describes each menu bar item, tool bar button, left panel and system panel contents in this screen.

Menu Bar	
System	**Exit:** Exit the program.
Security	**Change Password:** Change the password of the current user. **Logout:** Log out the current user.
Language	Specify the desired GUI language. * The language options will differ according to the language support on your operating system.
Help	**Help Contents:** Open the help web page. **About:** Display the program version.
Tool Bar	
MSN tool button	Open the *MSN Login and Configure* screen. This icon also indicates the MSN status (Green: MSN account is online; Red: MSN account is offline).
Left Panel	
IP input area	Enter the IP address of an agent.
Add button	Register the specified agent.
Structure tree	Display the registered agent and RAID system.
System Panel	
When an agent is selected: Display the current agent IP address, IP range field, and list of scanned registered RAID systems. **When a RAID system is selected:** Display the system information and event logs. See more information in the section **5.6.8 RAID System Monitoring on page 5-71**.	

5.6.7 RAID System Registration

You need to register RAID systems to RGC using the RGC GUI to build network connections to the RAID systems. Because the RGC Server communicates with RAID systems using RGC Agents, you also need to have one RGC Agent for each network of the RAID systems. After installing and running the RGC Agents, follow the steps below to complete the RAID system registration using the RGC GUI:

- Add the RGC Agents
- Scan the network of the RGC Agents to discover the RAID systems
- Register RAID systems

Add a RGC Agent

1. Enter the IP address of the Agent on the left panel of RGC GUI, and click the **Add** button.
2. An Agent icon ( ) with IP address will be displayed in the **Structure tree** section if the Agent has been successfully added.

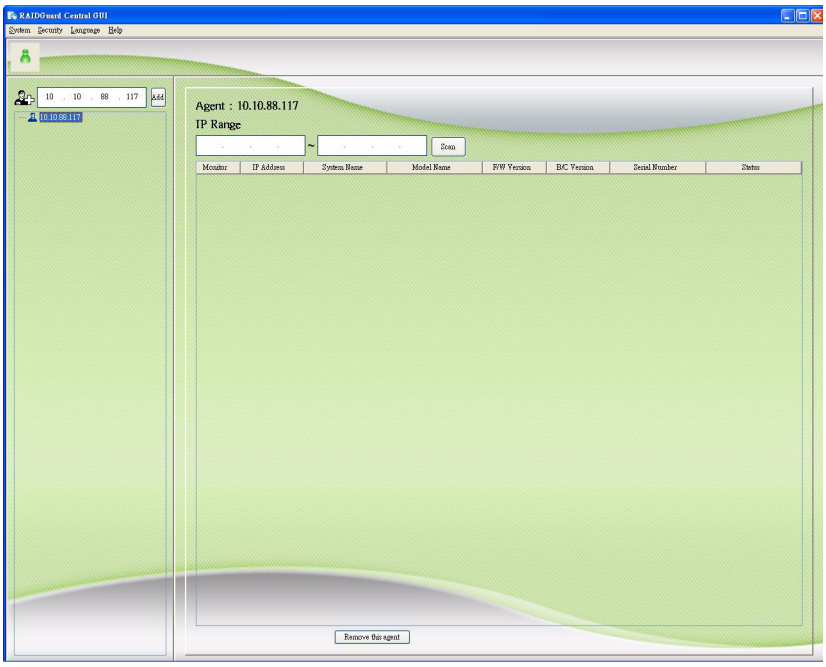


Figure 5-35 Adding the IP address of an agent

NOTE

1. If the RGC Agent is installed onto the local host server, you can also add it as one of the agents.
2. Each agent can only be controlled by a RGC Server.
3. The color of an agent icon ( ) will fade away when it goes offline.

Scan RAID systems

1. Click the Agent icon ( ) on the **Structure tree** section to choose the Agent.
2. Click the **Scan** button to discover the RAID systems on the sub-network of the Agent. If you want to scan a specific IP address range, enter the IP addresses in the **IP Range** field.

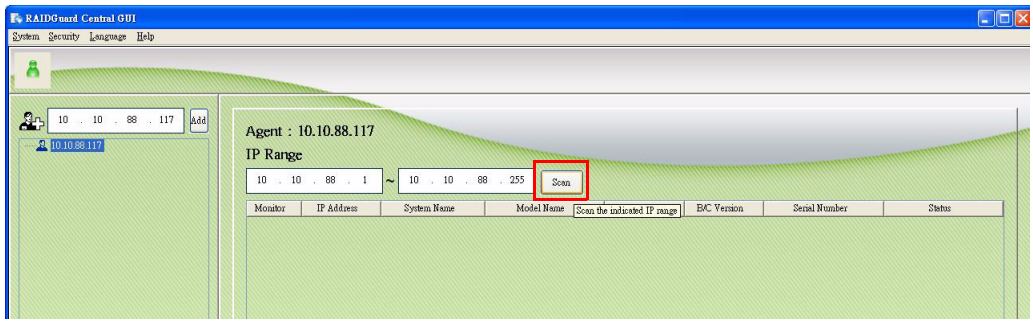


Figure 5-36 Scanning the online RAID systems in the specified IP range

3. For scanning RAID systems, the RGC Agent sends out broadcast packets on its subnet. If IP address range is specified, only the RAID systems within the IP address range will respond to the Agent. Up to 256 RAID systems can be displayed per scan. If you have more RAID systems on single subnetwork, you need to carry out multiple scans using different IP ranges.

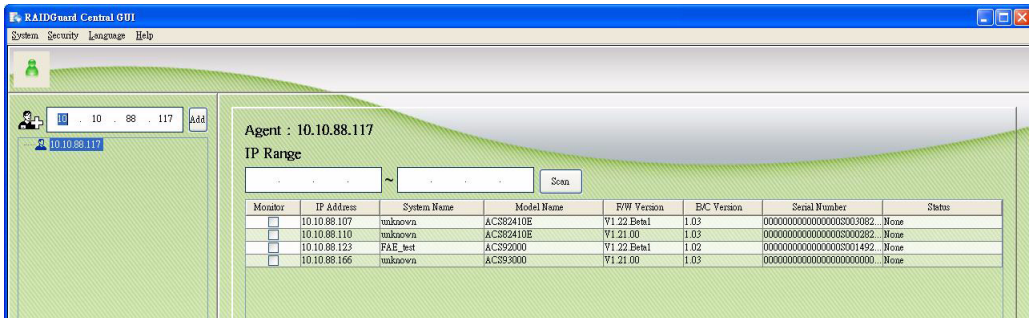


Figure 5-37 Scanning the online RAID systems in the selected agent's domain

Figure 5-37 shows the RAID system scan screen. The System Panel contains the following columns to display the information of each RAID system discovered.

- Monitor
- IP Address
- System Name
- Model Name
- F/W Version
- B/C (Boot Code) Version
- Serial Number
- Status

Table F-1 shows the meaning of the text displayed in the Status column and the corresponding RAID system icons in the **Structure tree** section.

Table 5-2 System status information

Icon	Status	Description
	None	Unregistered RAID system with unknown status.
	Normal	Registered online RAID system, functioning normally. Query thread queries the registered systems every ten seconds. Their statuses will be changed accordingly.
	Offline	Registered offline RAID system. The RGC cannot reach the RAID system because the RAID system or its network link is down. The system status will be returned back when it is restarted.
	Trouble	Registered defective RAID system. The RAID system requires your attention. The system will be changed to "Normal" after the beeper is disabled.

Register a RAID system

1. Login to RAID systems with admin is required for the registration. RAIDGuard Central will attempt to use the default admin password '0000' to login the selected RAID system. If the password is incorrect, it will pop up a window to request for your input.

NOTE

1. If you register the selected RAID system three times with the wrong password, the pop-up password request window will close. Re-select the RAID system you want to register and the pop-up window appears again.
2. If you have checked the checkbox to remember your password on the pop-up password request window. Once entered, the correct password of each RAID system is automatically stored on your computer so that you do not need to retype it every time you register and unregister the corresponding RAID systems. However, the changed password will be discarded the next time you launch the RAIDGuard Central.

3. After the registration is completed successfully, a RAID system icon together with the IP address of the RAID system will be added to the RGC Agent branch in the **Structure tree** section. **Figure 5-38** shows the updated screen after the registration of two RAID systems is complete.

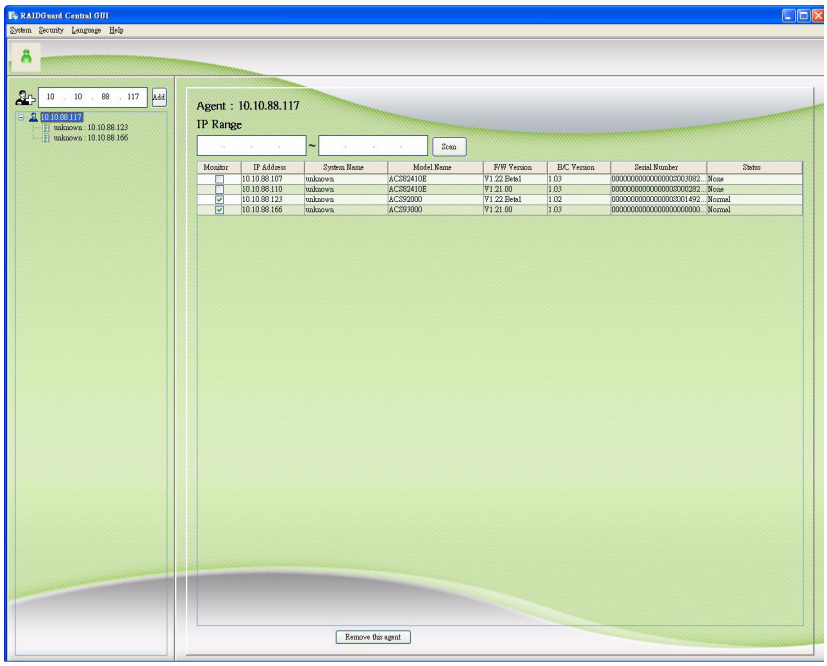


Figure 5-38 Registering a RAID system to an agent

Remove a RGC Agent

To remove an agent from the RGC Server, do the following:

1. Select the agent you want to remove from the structure tree.
2. Click the **Remove this agent** button in the system panel, and the selected agent is removed from the RGC Server.

NOTE

To clear the records of all RAID systems registered to a removed agent, you need to remove all RAID systems registered to this agent first before removing a RGC Agent. See the next section **"Unregister a RAID system"** for more information.

Unregister a RAID system

To remove a registered RAID system, uncheck the checkbox in the **Monitor** column for the RAID system you want to unregister from the RGC Agent.

NOTE

1. You can have a maximum of four users logged into a RAID system at any one time, irrespective of the service they are using. It means that a RAID system can be registered to up to a maximum of four agents if the RAID system is not logged in for other services.
2. When the removed agent is registered to the RGC Server again, all previously registered RAID systems will be also restored to the agent.

NOTE

3. Each RAID system has a default administer password, which is '0000.' This password is required when registering and unregistering a RAID system. If the password is changed, a password request window appears.

5.6.8 RAID System Monitoring

After the RAID systems are registered, the RAIDGuard Central will download the event logs from the RAID controller to local database. RAIDGuard Central will also start sending out query packets every ten seconds to check the status of the RAID systems. You may now do the following tasks by the RGC GUI:

1. View the event logs of a RAID system
2. Save the event logs of a RAID system to a file
3. Launch the web GUI of a RAID system

- **View the event logs of a RAID system**

Click a registered RAID system on the structure tree. The retrieved system information and existing event logs are displayed in the system panel.

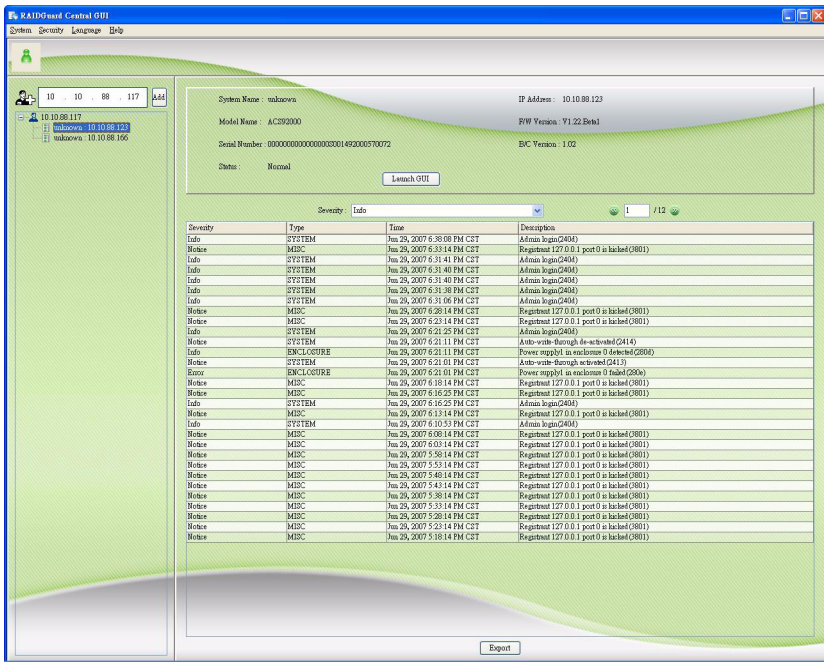


Figure 5-39 RGC GUI - System Panel

Click the **Severity** drop-down menu to display the event logs according to the specified severity level. You can view the event logs in different pages by either using the « and » buttons or entering the required page number in the page number field.

- **Export event logs**

  The **Export** button allows you to export all the stored event logs of the selected RAID system to a file. Click the **Export** button and the **Export Logs** window appears. Choose a directory where you want to save the export file, type the file name, and specify the file type to save it as an htm file.

- **Launch RAID system GUI**

  The **Launch GUI** button allows you to monitor the status and view the configurations of each RAID system on the remote server. To open the GUI of the current RAID system, click the **Launch GUI** button.

> **NOTE**
> The RGC Server and RGC Agent will use ports starting from 20000 to forward the transaction of web GUI access between a web browser and the RAID systems.

5.6.9 Configuring MSN Event Notification

The RAIDGuard Central integrates with the MSN service to notify users of system status changes by sending instant messages. Follow the steps below to configure this function:

1. From the Tool bar in RGC GUI, click the MSN tool button (or) to open the **MSN Login and Configure** screen.
2. Select the **Login** tab to enter the MSN account and password to be used by RAIDGuard Central to login to MSN server and send out messages.
3. Select the **Configure tab** to set up message recipients and severity level of the event logs to be sent. Up to 3 recipients can be configured.
4. After the MSN account and the recipients are configured properly, RAIDGuard Central will connect to MSN server and remain online. You may check the icon on the MSN button to see if the RAIDGuard Central is online (Green) or not (Red). For every 5 seconds, RGC will send out one message to notify the recipients of the latest events. Note that the messages will carry the events that happened in the past 30 minutes.

> **NOTE**
> RAIDGuard Central leverages TjMSNLib to support MSN notification, and it currently supports MSN Protocol (MSNP) version 11, and MSN clients version 7.0 or earlier. It does not support "offline message", so the recipient has to be online to get event notification messages.

* RAIDGuard Central uses TjMSNLib 5.0 as the MSN Messenger client library. TjMSNLib is an MSN Messenger client library, which is licensed under GPL (General Public License). For more information about TjMSNLib, please visit the TjMSN website at http://tjmsn.tomjudge.com/.

5.7 VDS Provider

5.7.1 Overview

The RAID controller supports Microsoft Virtual Disk Service (VDS) by supplying a VDS Provider. It allows you to use VDS-compliant software to manage the RAID systems on Windows platforms.VDS is a key component in Microsoft Simple SAN Solutions, and has been adopted by many leaders in the storage industry.

VDS is a management interface standard on Microsoft Windows for communication between storage management software and RAID hardware. You may manage RAID systems from different vendors by VDS-compliant software as long as VDS providers for the RAID systems are installed.

The architecture of VDS is illustrated as below:

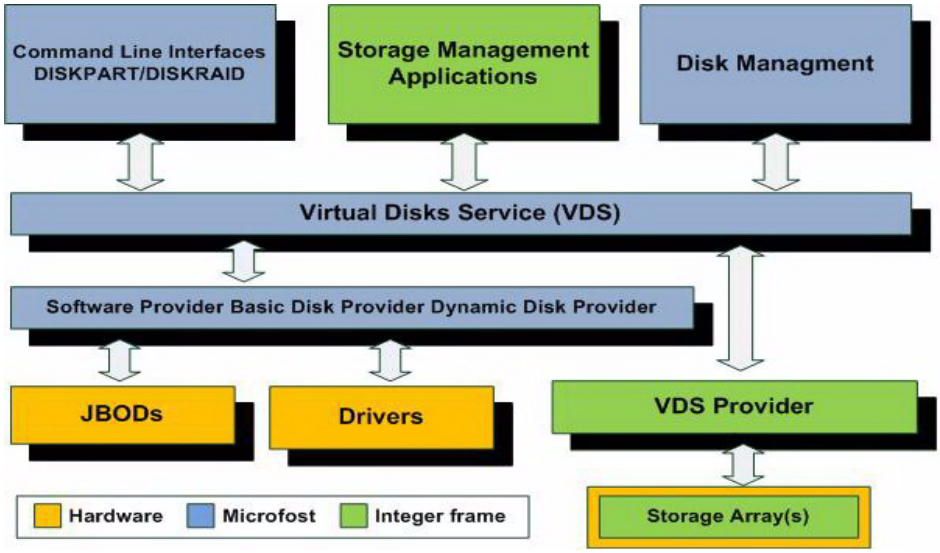


Figure 5-40 VDS Provider illustration

VDS is supported on Windows server 2003 SP-1(VDS1.0), Windows server 2003 R2 (VDS1.1), and Windows server 2008 (VDS1.1). Microsoft provides both command-line and GUI tool based on VDS: DiskRAID and Microsoft Storage Manager for SAN. VDS-compliant storage management software from other vendors is also available. Please see Section **G.5** for more information.

You may follow the steps below to build VDS-based management environment.

5. Install your RAID systems and connect them to networks.
6. Choose a management host system connected to the same LAN
7. Install the VDS Provider on the management host system.
8. Use VDS Provider Configuration Utility to locate the RAID systems and complete the registration for the VDS Provider

You may now start using VDS-compliant manage software to manage the registered RAID systems.

5.7.2 Installing the VDS Provider

Follow the steps below to install the VDS Provider onto the management host.

1. Copy the software file (VDSProvider_SW_1.00.zip) into the computer, and extract this file to a folder.
2. Double click the 'Setup.exe' file in the folder.
3. Follow the on-screen instructions to complete the installation.

NOTE

The VDS Provider Configuration Utility requires that you have Java Runtime Environment (JRE) version 1.5 or later installed on your Windows system.

5.7.3 Uninstalling the VDS Provider

Follow the steps below to uninstall the VDS Provider GUI from the management host.

1. Click Start > Settings > Control Panel > Add or Remove Programs.
2. Locate VDS Provider and click on it to start the un-installation. Click No to quit or Yes to confirm the un-installation.

5.7.4 Using the VDS Provider Configuration Utility

Before using VDS-based management for RAID systems, you are required to use the VDS Provider Configuration Utility to register the RAID systems such that the VDS Provider knows how to link to the RAID systems by network. You are also required to supply the password of the RAID systems for the VDS Provider to get proper management access rights to the RAID systems.

To launch the VDS Provider Configuration Utility, click **Start > Programs > VDS Provider > Configure Tool** (assuming the VDS Provider is installed in its default path). The table below describes the functions of the configuration utility.

Menu Bar	
System	**Exit:** Exit the program.
Help	**Help Contents:** Open the help web page. **About:** Display the program version.

Scan Bar	
Scan RAID systems in the LAN	Press the bar to scan the online RAID systems on the LAN and they will be displayed on the System Panel.
System Panel	
Display the information of RAID system.	

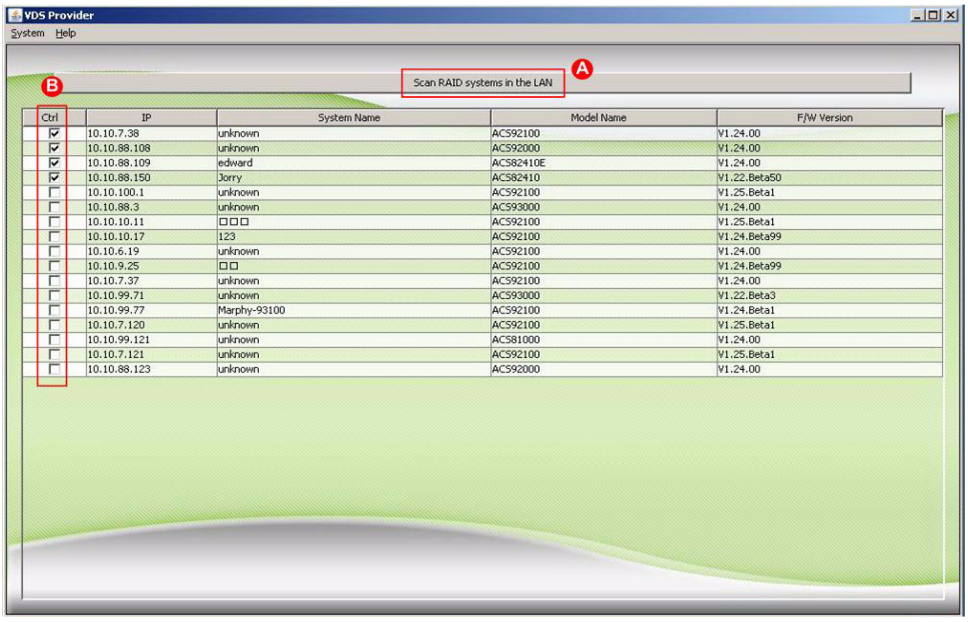


Figure 5-41 VDS Provider Configure screen

- Register RAID systems

1. Click the **Scan RAID systems in the LAN** button to locate RAID systems on the LAN.
2. Check the checkbox in the **Ctrl** column of the RAID system you want to register.
3. For each checked RAID system, a window pops up for you to enter the password.
4. If all setting are done, choose '**Exit**' to exit this program.

NOTE

1. At most 16 RAID systems are managed by single VDS Provider.
2. If the password of RAID systems is changed, you need also update the password for the VDS Provider by the Configuration Utility

5.7.5 VDS-Based RAID Management Software

- **Microsoft DiskRAID**

DiskRAID is scriptable command-line RAID management software supplied by Microsoft. After entering DiskRAID command prompt, you may use the "list provider" command to verify if the VDS Provider is properly installed, and use "list subsystem" command to see all RAID systems registered. See below for an example of using these two commands.

```
DISKRAID> list provider
  Prov ###  Name                                      Version     Type
  --------  ----------------------------------------  ----------  -------
  Prov 0    Accusys VDS Provider                      1.0         FC
DISKRAID> list subsystem
  Subsys ###  Name                          Status      Health
  ----------  ----------------------------  ----------  ----------
  Subsys 0    ACS82410                      Online      Healthy
```

Please follow the links below and enter "diskraid" to find more information:

Microsoft Web Site Links:

Search link: **http://search.microsoft.com/?mkt=en-US**

- **Microsoft Storage Manager for SANs**

The Storage Manager for SANs (SMfS) is RAID management GUI introduced in Windows Server 2003 R2 by Microsoft.

You may follow the steps below to install it:

1. In Control Panel, click **Add or Remove Programs**. Then click **Add/ Remove Windows Components**.
2. From the list of components, in the Windows Components Wizard dialog box, select **Management and Monitoring Tools**, and click **Details**.
3. From the list of subcomponents, select **Storage Manager for SANs**, and then click **OK**.
4. Click **Next**, and after the configuration of the new component has completed, click **Finish**.

For more information, please follow the link below:

Microsoft Web Site Links:

Search link: **http://technet2.microsoft.com/windowsserver/en/library/25257b2a-6d72-4adb-8f43-e3c0d28471d01033.mspx?mfr=true**

NOTE

You have to login as a member of the Backup Operators group or Administrators group on the local computer for using Microsoft VDS software.

- **Qlogic SANSurfer Express (VDS Manager)**

  Qlogic SANSurfer Express is a point-and-click GUI utility that allows administrators to discover supported Fibre Channel storage devices, including host bus adapters (HBAs), switch, and array systems. It also permits configuration and monitoring of these devices.

  For more information, please contact Qlogic or follow the link below:

  Web Site Links: http://www.qlogic.com/

- **Emulex EZPilot**

  EZPilot is an end-to-end storage provisioning application for deploying industry-leading solutions from Emulex and its partners. EZPilot features an intuitive storage manager GUI for discovery, allocation and assignment of storage in SAN. It also provides users with a comprehensive view of the SAN environment, graphically displaying all supported servers, HBAs, switches and storage.

  For more information, please contact Emulex or follow the link below:

  Web Site Links: http://www.emulex.com

Chapter 6: Troubleshooting

6.1 General Guidelines

When you encounter issues, the most essential troubleshooting is to check the event log of your RAID system and carry out the suggested actions offered in the Appendix D. In addition, you may need to check the system log of the operating system at your host computers.

Because there are a wide variety of hardware and software combinations, use the following checklist for problem determination:

- Check all cables to make sure they are connected properly
- Check all hardware units are powered on and working properly
- Check any recent changes in hardware, software, or configurations
- Verify that the latest version of firmware and software are used
- Verify that the latest version of BIOS and device driver of HBA are used
- Verify that the operating systems, HBAs, switches, transceivers, and hard disks are in the compatibility list
- Check how to reproduce the problems

Before you call support, please collect the related information above to assist the support staff in identifying the problems. It is also required to acquire the following three log files:

(1) RAID system user-level event log in human-readable form (**.csv** or **.txt**).

(2) RAID system diagnostic-level event log (**.bin**).

(3) the log file at operating system.

NOTE

The **.bin** log file is stored on hard disks, so please keep your hard disks in the system when downloading the log file. For redundant-controller systems, you're required to download the **.bin** log file for each controller.

6.2 Beeper

When the **Beeper Control** is set to **On** (see **2.9.5 Miscellaneous on page 2-66**), the system will turn on the beeper alarm if one of the following occurs. If the user mutes the beeper via CLI, LCD, or GUI, the system temporarily mutes the beeper until a new failure or error occurs.

- Voltage failure or error

- Power supply failure or error
- Fan failure or error
- Temperature failure or error
- BBM failure or error (when BBM is connected)
- Disk SMART warning
- Disk bad block over threshold warning
- Disk group with degraded logical disk and no disk for rebuilding
- Disk group with faulty logical disks
- UPS failure or error (when **UPS control** is on, see **2.9.4 UPS on page 2-66**)
- Controller failure or removed
- Dual controllers fail to boot up because of configuration conflict
- Controller failback cannot proceed

6.3 Performance Tuning

Performance tuning is always not an easy job because it requires in-depth knowledge of hardware and software. This section offers a few guidelines for you to identify performance problem sources and to do improvements. However, the system performance depends on not only the RAID system but also the capability of all software and hardware components along the I/O path. Please contact your solution providers to choose field-proven configurations.

1. Understand the I/O workload pattern

Understand your workload before configuring the RAID for your hard disks. Most applications can be classified into two types of workload: transaction (database or file server) and stream (video/audio or backup/archival). The former tends to be random access with variable IO size, and the former is sequential access with large IO size. Read the manual of your applications to find the suggested RAID configurations, or check the Appendix when choosing the RAID configurations.

2. Adjust the controller performance parameters

The RAID system is equipped with many parameters that allow you to gain excellent performance and also poor performance when poorly configured. Basically delayed write and read ahead option should be turned on, and cache unit size should be set according to your IO size. But if you are unsure about how the parameters work, please choose the performance profile in the Quick Setup menu (see **2.5 Quick Setup on page 2-19**) according to your workload or leave all parameters as default.

3. Use large I/O size at host

Aggregating multiple contiguous I/O into single I/O of big size significantly improves the sequential-I/O performance because of better bandwidth utilization and reduced CPU loading. You can use larger allocation size (a.k.a. block size) when creating a file system (for example, 64KB for NTFS and Apple Xsan, and 4KB for ext3). If you want to use multiple I/O connections, multi-path I/O is more advised than software striping (RAID 0), since the later tends to limit the maximum I/O size of single I/O access. But if you still need software striping, use the maximum stripe size (for example, 256KB for MAC OS striping breadth). There could be also options provided by the operating systems and HBA drivers for you to increase the maximum I/O size.

4. Ensure aligned I/O access

The RAID controller can process I/O requests more efficiently if I/O is aligned with the RAID stripe size or cache unit size. For x86 systems, file data of a file system (like NTFS) starts after the MBR (Master Boot Record), which occupies the first 63 sectors of a LUN (see **2.6 RAID Management on page 2-21**). So, the alignment offset option of a LUN is needed to set (63 or 191 sectors for NTFS). However, it works only for your first partition in a LUN. When creating partitions on Windows 2003 and later, you may use the Disk Partition Toll (Dispart.exe) with the option **align=N** to force the partition to start at the specified alignment offset. To ensure all data chunks are aligned, you need also to make the NTFS allocation size equal to or bigger than the RAID stripe size.

5. Ensure I/O access fits striping data size

When you set the write cache of a RAID5 LUN as write-through, data written to only a stripe of a RAID5 data row causes reading the old data and parity to calculate the new parity is necessary. But if all the stripes of a data row are written with new data, then the new parity can be produced with only the new data. An example to do so is the option **–E stride=N** of Linux ext3 file system, and you can set the N as 64 for a ext3 LUN with 4KB allocation size on a 4-disk RAID0 LUN with 64KB stripe size (64 = 4 x 64k/4k).

6. Check RAID system health status

Browse the monitoring web page (see **2.2 Monitor Mode on page 2-5**) and the event log (see **2.9 Event Management on page 2-61**) to make sure your systems are in a good shape. Problems like bad blocks, bad hard disks, poor cabling, or incompatible devices hurt performance because the RAID controller wastes its energy doing error recovery. Also note that when the auto-write-through option (see **2.9.5 Miscellaneous on page 2-66**) is turned on, failure of power supply units, BBM, or so would force the delayed-write option to be off.

7. Check I/O path connections

You have to make sure the bandwidth of I/O path can deliver the performance you need. For example, if you install a quad-port 4Gbps Fibre Channel HBA to a 4-lane PCIe 1.0 slot, your bandwidth will be limited

to 1GB/s bandwidth of the PCIe slot. You need also to check the data rate of I/O paths is configured properly without degradation. For example, your 4Gbps Fibre Channel channels are configured to run at 2Gbps rate, you need to check HBAs, switch, host interface ports, and disk interface ports of the RAID system.

8. Check hard disk settings

Hard disks are the destination of all I/O and thus also important to performance. For hard disks that have variable data rate (like 1.5 Gbps or 3 Gbps for SATA disks), please make sure the setting is correct by checking the jumpers on the hard disk. You need also to make sure the on-disk cache is turned on (see **2.8.1 Hard disks on page 2-56**). Lastly, the performance of hard disks varies from model to model, and even the hard disk firmware revision could also cause differences, having the latest revision helps you to get better performance.

9. Add memory at host computer or RAID controller

Adding more memory to your motherboard or RAID controller helps to cache more data at memory to so as to reduce the number I/O access to hard disks, especially helpful for data being accessed frequently. Bigger memory also helps to avoid the performance glitch because more data can be buffered for write commands or pre-fetched for read commands, especially helpful for multiple video streams.

10. Check data layout on hard disks

A hard disk can deliver its best performance when servicing I/O access on the inner tracks of disks, which provides data of lower block address (LBA). As a result, to deliver high-throughput performance, place the data in the beginning area of disk groups. To retain the performance of data at the second half area of disk groups, you may use more hard disks with striping.

11. Make the I/O workload distribute evenly

Check below to ensure the I/O workload are distributed evenly

- Data is transferred evenly through multiple host-interface connections
- MPIO is enabled and dynamic load balancing is turned on
- I/O are processed evenly by the two controllers
- I/O are distributed evenly to multiple disk groups

12. Close the web GUI during I/O access

Sometimes, the web GUI or RAID monitoring software could be an influential factor to the performance unstableness, because it needs to retrieve RAID system status periodically, and consumes CPU cycles of the storage processor. Close the web GUI when you run time-sensitive applications.

13. Reduce the impact of background task

The background I/O tasks, like RAID initialization or rebuilding, have impact to the performance of your applications, because they need to access hard disks. Even SMART monitoring could cause disturbance. You may set the priority of background tasks to low, or schedule these tasks to run at non-business hours to avoid the impact.

14. Constantly monitor the I/O statistics

To know details of the performance of your RAID system, you may check the performance management web pages, by which you may identify slow hard disks, slow host interface links, or unbalanced workload distribution (see **2.11 Performance Management on page 2-76**). Some operating systems offer similar utilities. For example, Microsoft Windows Performance Monitor not only displays many useful statistics but also can be configured to send out alerts according to the threshold you set. The statistics can also be saved as a log file. You may find similar utilities from your HBA and switch vendors.

15. Know more about performance benchmarking

And finally, you have to understand that the test result of performance benchmark tool is not always related to your real-world performance. You have to be careful with choose right tools and right testing workload profiles to mimic your application behaviors.

6.4 Hard Disks

Hard disks are the most important components in a RAID system because they are where the data resides. Please contact your RAID system supplier to get the list of qualified hard disk models when you're choosing hard disks.

1. Hard disks cannot be recognized by the RAID controller

The hard disks are initialized by the RAID controller when the controller boots up or when the hard disks are plugged into the RAID system. If a hard disk cannot be ready within a specific period of time during the initialization, the RAID controller will force the hard disks enter faulty state and you cannot see any model information of hard disks. To ensure hard disks have enough time for power-on, you may extend the delay time when boot-up of the RAID controller (see **2.8.1 Hard disks on page 2-56**).

2. Hard disks are offline unexpected

The RAID controller takes a hard disk offline when the hard disk cannot respond to the RAID controller after the full-cycle error recovery procedure has been done. This could happen when the hard disk is permanently dead because of its internal component failure, and you lose all your data on the hard disk. Another reason a hard disk is taken offline is that its reserved space for meta-data (RAID configurations) cannot be written, which means the reserved space for bad block

reallocation in the hard disk has been full. This is unlikely to happen because two copies of meta-data are reserved, and a hard disk is offline only when both areas cannot be accessed.

An offline hard disk might also be transiently down because of its disk controller firmware lockdown or mechanical unstableness. In this case, the hard disk is still accessible and you may reuse it, but the hard disk might fail again.

3. Verify hard disk health status

To know exactly if a hard disk fails or not, using SMART check or DST (Device Self-Test) to test the hard disks in question is a good choice. It's also advised to check the number of bad blocks and warning events reported by the RAID controller (see **2.8.1 Hard disks on page 2-56**). Another indicator to the health condition of a hard disk is its I/O response time, because out-of-specification response time could be caused by abnormal error recovery procedures (see **2.11.1 Hard disks on page 2-76**).

4. Adjust hard disk settings

Tweaking the hard disk-related settings could help to accommodate the exceptional behaviors of hard disks (see **2.8.1 Hard disks on page 2-56**). The following are some common workarounds:

- Extend **Disk I/O Timeout** to accommodate slow disk operation
- Increase **Disk I/O Retry Time** to try I/O more times before giving up
- Reduce **Transfer Speed** to mitigate bad signal quality of disks
- Disable **I/O Queue** to avoid problematic NCQ support of disks
- Disable **Disk Standby Mode** to avoid problematic sleep support of disks
- Extend **Disk Access Delay Time** to allow longer time for disk spin-up

5. Check failure of multiple hard disks

If multiple hard disks are taken offline at a time, it could be system-level problem. For example, if the hard disks in a JBOD system are offline unexpected, poor cabling in SAS or FC expansion chain would also lead to unexpected hard disk offline. In addition, poor heat ventilation, unstable power supply, or hardware quality issues could also lead to offline of multiple hard disks. In case there are multiple failed hard disks causing corrupted logical disks, you may try to use array recovery utility to the RAID configurations (see **2.7.13 Array recovery on page 2-52**).

6. Ensure proper power on/off sequence of RAID and JBOD

You have to make sure the expansion chassis has been ready before powering on the RAID system, such that the RAID system can properly recognize the expansion chassis and the hard disks. And shut down the

RAID system first and then its expansion chassis, such that the RAID systems won't see the lost of expansion chassis as a failure event.

7. AAMUX boards are required for attaching SATA drives to SAS systems

An AAMUX board is required SATA hard disks installed in SAS JBOD systems and for redundant-controller systems. AAMUX provides dual paths for controllers to access single-ported SATA drives. Check your RAID system hardware manual for more details, and contact your RAID system supplier to get the AAMUX boards.

8. Regular maintenance helps to avoid disaster

To avoid performance degradation or data loss caused by failed hard disks, it's advised to enable periodical SMART checking, automatic disk cloning, and periodical disk scrubbing. Please also set up spare disks for such that disk rebuilding can be started right away when any hard disks fail.

6.5 User Interfaces

1. The Web GUI cannot be connected

You can use the Web GUI and other network-related management features (including the host-side management software) only when the management network interface is configured properly. Please check if the LED indicators of the Ethernet port are lit up properly (refer to the hardware manual for details), and the IP address has to be set to enable the network interface. You can manually set the IP address by the LCD or local CLI, or use a DHCP server on the network.

2. Some user operations are prohibited

Each user operation can be executed assuming some sort of conditions, please check Chapter 2 to find out the restrictions of your operations. The web GUI will also offer information and suggestions when a user operation cannot be done. A few common guidelines and examples are as below:

- To avoid mistakenly destroying data, a disk group cannot be deleted when it contain logical disks.
- To avoid overloading, disk scrubbing is not allowed for a degraded disk group, or an initializing disk group.
- To avoid confusing operations, some settings cannot be modified when a related state happens. For example, rebuilding-related settings cannot be modified when there is rebuilding disk.

3. The web GUI does not show updated information

The web browser displays the cached the web pages such that you cannot see the updated web pages. For example, the percentage of

firmware upload progress isn't updated. Please go to the setting page of your web browser to delete the temporary files, cookies, and the history.

4. It takes very long time for the web GUI to respond my commands

The web GUI is presented by browser but its contents are generated by the storage processor, which need also process I/O request as well as other maintenance tasks. You might experience slow GUI when the I/O access is very heavy. Please reduce the workload or stop some background tasks.

Bad hard disks or bad blocks could cause long response time of web GUI, because some system information is retrieved from or written to hard disks. When it takes a long time for hard disks to complete an I/O request, the web GUI would freeze to wait for the I/O completion. Please use hard disk diagnostics utilities to identify the problematic hard disks and remove them.

5. Some pages in the System Management menu are not viewable

The RAID controller offers two levels of administration access right. If you login as a user (username: user), you are restricted to read-only web GUI pages. Login as administrator (username: admin) allows full-function management and access to all pages.

6. No display or response on the LCD

If your RAID system is capable of redundant-controller configuration, the LCD can be managed by only one of the two controllers at a time, and you need to use LCD hot keys (see **3.2.5 Hotkeys on page 3-5**) to choose a controller to control the LCD.

6.6 RAID Configuration and Maintenance

1. 2TB limitation and how to choose sector size

Because of 32-bit logical block addressing (2^32 x 512 bytes = 2TB) used by the MBR-based partition table and by the host operating systems, like Windows 2000, Windows XP 32-bit, and Linux 2.4.x kernel, the maximum size of single partition or logical drive is limited to 2TB size. You can use logical volume management (LVM) software to aggregate multiple LUNs.

For Windows above to work around the 2TB limitation, choose bigger sector size of a LUN (see **2.6.7 Storage provisioning on page 2-36**). However, you cannot use dynamic disk in Windows for the LUN with non-

512B sector size, and your data will be lost if you change the sector size of a LUN. The table below shows the capacity correlated with sector size.

Table 6-1 The capacity correlated with sector size

Sector size	512B	1KB	2KB	4KB
LUN Size	0 ~ 2 TB	2 ~ 4 TB	4 ~ 8 TB	8 ~ 16 TB

The latest partition table GPT (GUID Partition Table) and modern operating systems, like Windows XP 64-bit, Windows 2003 server SP1, Windows 2008 server, Windows Vista, and Linux 2.6.x kernel, support 64-bit logical block addressing without the 2TB limitation. Using 512B as the sector size (default) is fine.

2. Failed hard disk interrupts the background maintenance tasks

To avoid unwanted overloading and risk, the reconfiguration task of a disk group is paused and the disk scrubbing is aborted when a hard disk of the disk group goes offline. If there is a spare disk or the failed hard disk is replaced, the reconfiguration can be resumed after the disk data rebuilding is done. For disk scrubbing, you'll need to restart it manually.

3. Failed hard disk interrupts the background maintenance tasks

To avoid unwanted overloading and risk, the reconfiguration task of a disk group is paused and the disk scrubbing is aborted when a hard disk of the disk group goes offline. If there is a spare disk or the failed hard disk is replaced, the reconfiguration can be resumed after the disk data rebuilding is done. For disk scrubbing, you'll need to restart it manually.

4. Hard disk shows Unknown state

The configurations on the hard disks cannot be recognized by the controller. You need to erase the configuration information on the hard disks for your RAID system to use the hard disks.

If you need not to retain the data and the configurations on the hard disks, you can clear configurations on the hard disks (see **2.10.1 Restoring to factory settings on page 2-67**). You may also turn off the On-line Array Roaming option (See **2.7.16 Miscellaneous on page 2-55**). With that, the RAID controller will not check the stored configuration information of hard disks and see any newly installed hard disks as hard disks without configurations. You may remove and then re-install the unknown hard disks to the system (either manually or by GUI, **2.6.1 Hard disks on page 2-21**). The hard disk state will return to "Unused" state.

If you need your data and configurations, please contact your system supplier for solutions.

5. Hard disk shows Conflict state

The Conflict state indicates that the hard disk contains valid RAID configurations but the controller cannot work with such configurations.

If the conflict is because the cache unit size of the controller is bigger than the stripe size of the logical disk on the hard disks, you can change the cache unit size (see **2.7.16 Miscellaneous on page 2-55**) and restart the system to accommodate the logical disk. The cache management algorithm requires that the cache unit size has to be equal to or smaller than the stripe size of any logical disks managed by the RAID controller.

The conflict might also be because there has been a disk group with the same disk group ID of the hard disks. You can use Array Roaming Utilities (see **2.7.12 Array roaming on page 2-51**) to import the hard disks to form a disk group with a new disk group ID.

Other configuration conflicts might be caused incompatible firmware version. You're required to erase the configuration information on the hard disks for your RAID system to use the hard disks. Or, contact your system supplier for solutions.

6. Disk group enters degraded mode.

Make sure that there are member disks available. Use the Array Recovery Utility to restore the disks to the degraded disk group (see **2.7.13 Array recovery on page 2-52**).

7. Faulty logical disks or volumes cannot be recovered

You are required to recover a disk group before recovering its logical disks. And similarly, to recover a volume, you're required to recover its logical disks.

6.7 Redundant Controller and MPIO

1. The replacement controller stops boot-up with LCD messages

When a replacement controller is online installed to the RAID system, the two controllers will synchronize with each other. If there is configuration conflict discovered (see Section 5.2), the replacement controller will stop boot-up. The beeper alerts, and the LCD shows the following messages:

(A) **CONTR MOD UNEQ**: the two controllers are of different model

(B) **DB UNEQ**: the two controllers have different daughter board

(C) **PLD VERS UNEQ**: the two controllers have different PLD version

(D) **MEM SZ UNEQ**: the two controllers install memory of different size

(E) **BBM INSTL UNEQ**: one controller has BBM, while the other has no BBM

Below list the resolutions for the configuration conflict.

(A/B/C) Contact your RAID system supplier to get the correct controller

(D/E) Install proper memory module and BBM

If the conflict configuration can be resolved by overwriting the configuration of the replacement controller, the following LCD messages will be displayed and waiting for your confirmation by LCD ENT button:

(F) **CHK BC VERS**: the two controllers have different boot code version

(G) **CHK FW VERS**: the two controllers have different firmware code version

(H) **CHK BBM OPT**: the two controllers have different BBM option

(I) **CHK ENC SN**: the two controllers belong to different enclosures

For (F) and (G), press the ENT button on the LCD to update the boot code and firmware code, respectively, and the replacement controller will reboot. For (H) and (I), press the ENT button to overwrite the BBM and enclosure serial number, and the replacement controller will continue boot-up.

2. During dual-controller boot-up, the controllers hang with LCD messages

When the two controllers boot up at the same time, negotiation will be performed between the two controllers to choose one controller as the master controller, and the other controller will follow the configurations of the master controller. The negotiation cannot be done if there is configuration conflict between the two controllers (see **5.3 Redundant Controller on page 5-21**). The controllers will stop boot-up to show messages on the LCD. The messages and corresponding resolutions are the same as failure of replacement controller.

If the two controllers have different versions of boot code or firmware, you need to choose between the versions. If the two controllers have different BBM option, you need to choose to enable or disable it. If **ENC SN UNEQ** is displayed, the two controllers came from different chassis, and you need to boot up first with only one controller as the master controller, and install the other controller later.

3. Host computer reports I/O errors during path/ controller failover

If you use MPIO against path or controller failure, it is essential to check if your MPIO driver is installed properly. Below are the checking items you need to do:

- A virtual disk has been mapped to LUNs of all host-interface ports in simple storage presentation configuration. Or, a virtual disk has been mapped to a host or host group in symmetric storage presentation configuration.

- Because a LUN is not accessible during regular initialization. Install the MPIO driver after the regular initialization of a virtual disk is done, or use background initialization.
- All cables are connected and the corresponding paths are displayed by the MPIO software utility.
- Check the device nodes from the operating system disk management utility to make sure the MPIO devices have been created. Make sure the number of MPIO devices matches your cabling topology (see **5.1 Multi-Path IO Solutions on page 5-1** for how to calculate the number).

4. The replacement controller cannot work for controller fail back

The replacement controller stops boot-up if it fails to discover the same set of expansion chassis of the surviving controller. You need to make sure the expansion chassis are properly attached to the expansion port of the replacement controller and there is no broken connection between the expansion chassis. Please also note that the I/O access and background tasks can be migrated to the replacement controller only after the host-interfaces of the replacement controller are properly connected to the host computers.

5. It takes too much time for path or controller failover with MPIO driver

The MPIO driver detects path failure by checking the HBA driver to get the link status. The setting of HBA determines how much time it takes for the MPIO driver to detect path failure and to do path failover. If your controller failover/failback is supported by MPIO drivers, it also determines how much time it takes for controller failover.

- Qlogic FC HBA BIOS Utility:

  Fast!UTIL > Advanced Adapter Settings > Link Down Timeout

  Fast!UTIL > Advanced Adapter Settings > Port Down Retry Count

- LSI FC HBA LSI command-line Utility: **LSIUtil > Change FC Port settings > Initiator Device Timeout**

Contact your HBA vendor for more information about these settings.

6. Linux pauses for a while during boot-up with dual-controller system

Because it takes time for Linux to test the standby LUNs of a controller, you might experience long boot-up time of Linux, but it hurts nothing after the Linux is running. If you want to reduce the boot-up time, please follow the procedures below after completing the installation of multi-path driver:

- Edit **/etc/modprobe.conf** (RedHat) or **/etc/modprobe.conf.local** (SUSE 10) to add this line:

  options scsi_mod dev_flags=Accusys:ACS92102:0x1000.

- Change to the **/boot** directory, and build the ramdisk image with the following command: **mkinitrd -f initrd-2.6.[kernel_version].img [kernel_version]** (RedHat), or **mkinitrd** (SUSE 10)
- Reboot the Linux system

7. Constant path failover or many disk timeout errors reported at host

Under heavy I/O loading, the operating systems might experience long I/O response time and falsely report I/O error when the response time is over its I/O timeout value. The MPIO driver might also be informed of I/O or path failure and the preferred I/O path would be changed constantly. This would severely hurt the performance. Extending the I/O timeout value of your OS or applications can mitigate this problem. For example, on Windows system, it is advised to set the registry key below to 60 or 90 seconds:
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Disk\TimeOutValue.

Appendix A: Understanding RAID

A.1 RAID Overview

The controller supports eleven types of RAID: RAID 0, 1, 3, 5, 6, 10, 30, 50, 60, JBOD and NRAID. The application(s) you are using will determine which RAID setup is best for you.

- **RAID Level 0**

  This level offers high transfer rates and is ideal for large blocks of data where speed is of the essence. Computer Aided Design, graphics, scientific computing, image, and multimedia applications are all good examples. If one drive in a RAID 0 array fails, the entire data array is lost.

- **RAID Level 1**

  This level may be an appropriate choice if cost and performance are of significantly less importance than fault tolerance and reliability.

- **RAID Level 3**

  This level is similar to the more commonly used level 5. Both offer a good level of fault tolerance and overall system reliability at a reasonable cost for redundancy overhead. RAID 3 is useful for large file sequential writes such as video applications.

- **RAID Level 5**

  This level offers high I/O transaction rates and is the ideal choice when used with on-line transaction processing applications, such as those used in banks, insurance companies, hospitals, and all manner of office environments. These applications typically perform large numbers of concurrent requests, each of which makes a small number of disk accesses. If one drive in a RAID level 5 array fails, the lost data can be rebuilt from data on the functioning disks.

- **RAID Level 6**

  This level is similar to level 5. Data is striped across all member disks and parity is striped across all member disks, but RAID 6 has two-dimensional parities, so it can tolerate double-disk failure.

- **JBOD ("Just a Bunch of Disks")**

  This is a method of arranging multiple disks and, technically, is not RAID. Under JBOD, all disks are treated as a single volume and data is "spanned" across them. JBOD provides no fault tolerance or performance improvements over the independent use of its constituent drives.

- **NRAID ("None RAID")**

  This level allows you to combine the capacity of all drives and does not suffer from data redundancy.

- **RAID Level 10**

  This level offers a compromise between the reliability and tolerance of level 1 and the high transfer rates provided by level 0.

- **RAID Level 30/50/60**

  RAID 30/50/60 performs striping over RAID 3/5/6 groups. With multiple independent RAID groups, performance and reliability can be improved. These RAID levels are supported by data striping volumes over logical disks.

A.2 RAID 0

RAID 0 links each drive in the array to form one large drive. Storage capacity is determined by the smallest drive in the array. This capacity is then applied to format all other drives in the array. When using a 40GB, 50GB and a 60GB drive in a RAID 0 array, your system will effectively have a single 120GB drive (40GB x 3).

RAID 0: Striped disk array without fault tolerance

Characteristics

- Storage capacity = (number of disks) x (capacity of the smallest disk)
- A minimum of two disks are required.
- Fault tolerance: No
- RAID 0 implements a striped disk array, the data is broken down into blocks and each block is written to a separate disk drive.
- I/O performance is greatly improved by spreading the I/O load across many channels and drives.
- No parity calculation is required, freeing up system resources.
- Fastest and most efficient array type but offers no fault tolerance.

Recommended use

- Video production and editing
- Image editing
- Pre-press applications
- Any application requiring high bandwidth

The following diagram illustrates writing data to a RAID 0 array composed of four HDDs connected to the controller. Data blocks are distributed across all disks in the array.

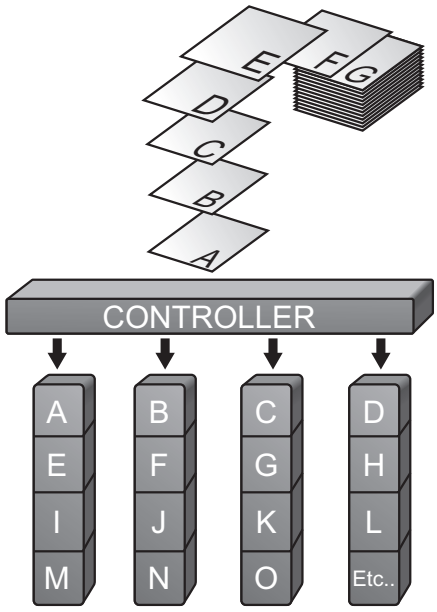


Figure A-1 RAID 0 disk array

A.3 RAID 1

RAID 1 is commonly referred to as *disk mirroring* as all data is duplicated on two or more disks. This provides a high access rate and very high data availability. RAID 1 has low performance for write operations but very high performance for intensive read operations.

RAID 1: Mirroring

Characteristics

- Storage capacity = the capacity of the smallest disk
- A minimum of two disks are required.
- Fault tolerance: Very good
- Read transaction rate: Good. Better than a single drive but worse than many other RAID levels.
- Write transaction rate: Worse than a single drive, but better than many other RAID levels
- 100% data redundancy means that in the event of disk failure, data can be copied directly to the replacement without rebuilding.
- All the disks contain the same data.

Recommended use

- Accounting
- Payroll
- Finance
- Any application requiring high availability

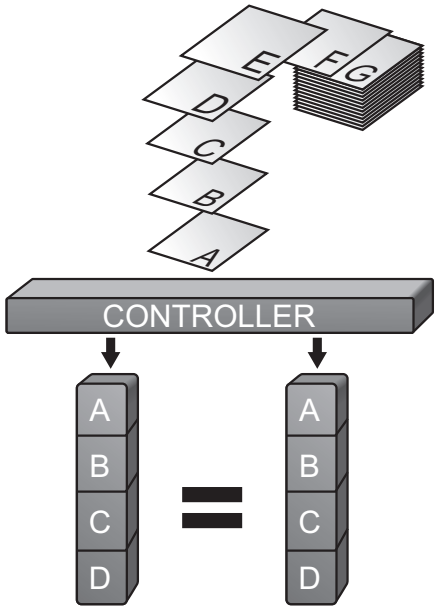


Figure A-2 RAID 1 disk array

A.4 RAID 3

In RAID 3, all data is divided into pieces, after which the system calculates the parity of these pieces. The pieces are written to separate disks in parallel with the writing of the parity data. In the event of disk failure, the parity data can be used to rebuild the lost data. If two or more disks fail, data will be lost. While the low ratio of parity disks to data disks ensures high efficiency, the parity disk is accessed more frequently than other disks, therefore making it unsuitable for random write access.

RAID 3: Parallel transfer with parity

Characteristics

- Storage capacity = (number of disks -1) x (capacity of the smallest disk)
- A minimum of three disks are required.
- Fault tolerance: Good
- The data block is striped, written on the data disks. Stripe activity is generated on writes, recorded on the parity disk and checked on reads.
- Low ratio of (parity) disks to data disks ensures high efficiency.

Recommended use

- Video production and live streaming
- Image editing
- Video editing
- Any application requiring high throughput

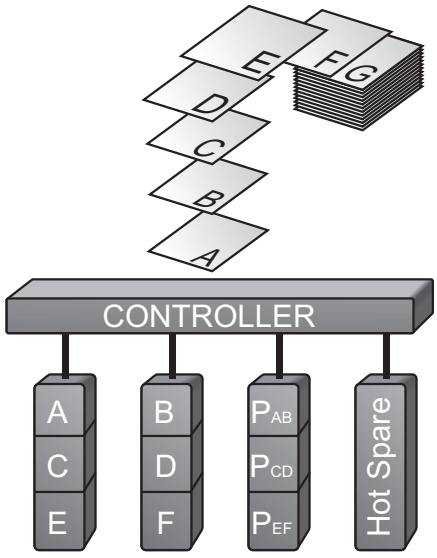


Figure A-3 RAID 3 disk array

A.5 RAID 5

With RAID 5, the system calculates parity from data on three drives. If one of the drives fails, parity data can be used to rebuild the lost data. Under RAID 5, parity data is stored across all disks in the array. This maximizes the amount of storage capacity available from all drives in the array while still providing data redundancy. Data under RAID 5 is block-interleaved.

RAID 5: Independent data disks with distributed parity blocks

Characteristics

- Storage capacity = (number of disks -1) x (capacity of the smallest disk)
- A minimum of three disks are required.
- Fault tolerance: Good
- Each data block is written to a disk. The parity of blocks with the same rank is generated on writes, recorded in a distributed location and checked on reads.
- Highest read data transfer rate, medium write data transfer rate
- Relatively low ration of (parity) disks to data disks results in high efficiency.
- Good aggregate transfer rate
- Most versatile RAID level

Recommended use

- File and application servers
- Database servers
- Internet, email and news servers
- Intranet servers

The diagram below represents the writing of data on a RAID 5 array composed of four HDDs connected to the controller. Parity blocks are represented by the letter P.

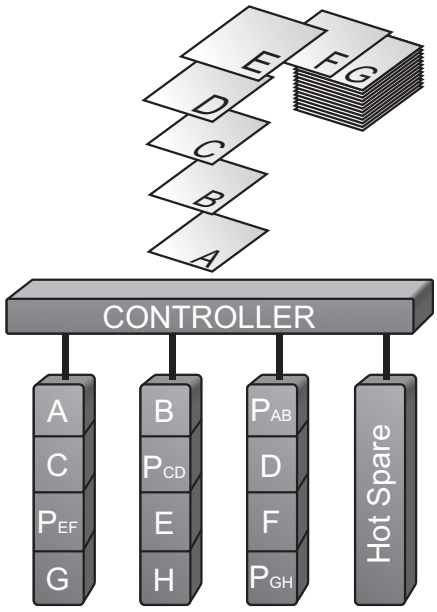


Figure A-4 RAID 5 disk array

A.6 RAID 6

RAID 6 stripes data and parity data across an array of drives, as with RAID 5, and calculates two sets of parity information for each stripe to improve fault tolerance. Performance-wise, RAID 6 is generally slightly worse than RAID 5 in terms of writes, due to the extra parity calculations. It may, however, be slightly faster in terms of random reads, due to the spreading of data over one more disk. As with RAID 3 and RAID 5, performance can be adjusted by changing stripe size.

RAID 6: Independent data disks with double parity blocks

Characteristics

- Storage capacity = (number of disks -2) x (capacity of the smallest disk)
- A minimum of four disks are required.
- Fault tolerance: very good to excellent
- Good speed with random reads

Recommended use

- File and application servers
- Database servers
- Internet, email and news servers
- Intranet servers
- Use in high reliability server environments

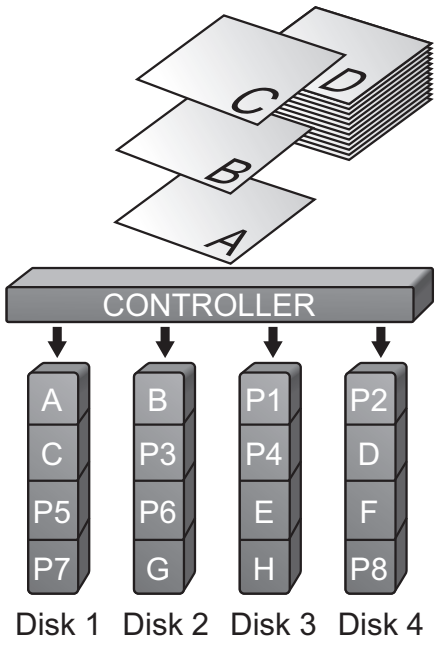


Figure A-5 RAID 6 disk array

A.7 RAID 10

RAID 10 arrays are formed by striping data across RAID 1 sub-arrays. This offers better performance than RAID 1 alone but does not have the speed of a pure RAID 0 array. Storage efficiency and fault tolerance vary depending on the number and size of sub-arrays compared to the array as a whole.

RAID 10: High reliability setup combined with high performance

Characteristics

- Storage capacity = (number of disks/ 2) x (capacity of the smallest disk)
- A minimum of four disks are required.
- Same fault tolerance as RAID 1
- I/O rates are high thanks to striping RAID 1 segments
- Can handle multiple simultaneous disk failures

Recommended use

- High performance database servers

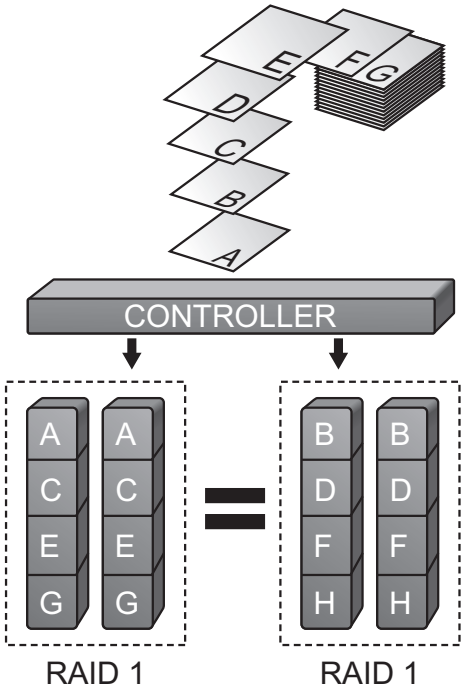


Figure A-6 RAID 10 disk array

A.8 RAID 30

RAID 30 arrays are formed by striping data across RAID 3 sub-arrays. This offers better performance than RAID 3 alone but does not have the speed of a pure RAID 0 array. Storage efficiency and fault tolerance vary depending on the number and size of sub-arrays compared to the array as a whole. RAID 30 resembles RAID 50 in terms of characteristics but is more suitable for handling large files.

RAID 30: Byte striping with parity combined with block striping

Characteristics

- Storage capacity = [(number of disks in each subarray) -1] x (number of subarrays) x (capacity of the smallest disk)
- A minimum of six disks are required.
- Good fault tolerance, in general
- Increased capacity and performance compared to RAID 3

Recommended use

- Multimedia
- File servers
- Large databases

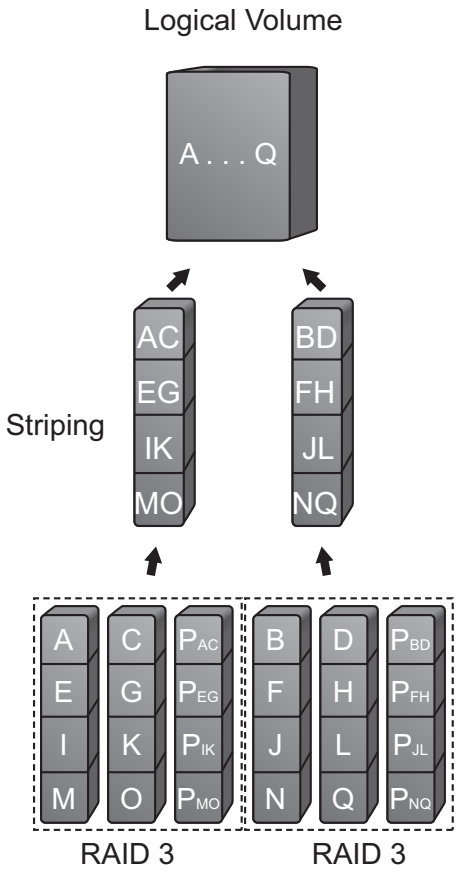


Figure A-7 RAID 30 disk array

A.9 RAID 50

RAID 50 arrays are formed by striping data across RAID 5 sub-arrays. Striping helps increase capacity and performance without adding disks to each RAID 5 array (which will decrease data availability and affect performance when running in a degraded mode). Storage efficiency and fault tolerance vary, depending on the number and size of the sub-arrays compared to the array as a whole. As mentioned above, RAID 50 is similar to RAID 30 in terms of characteristics but is more suitable for use with smaller files.

RAID 50: Block striping with distributed parity combined with block striping

Characteristics

- Storage capacity = [(number of disks in each subarray) -1] x (number of subarrays) x (capacity of the smallest disk)
- A minimum of six disks are required.
- More fault tolerant than RAID 5
- High data transfer rate
- RAID 0 striping ensures high I/O rates

Recommended use

- Applications requiring random positioning performance
- Large databases

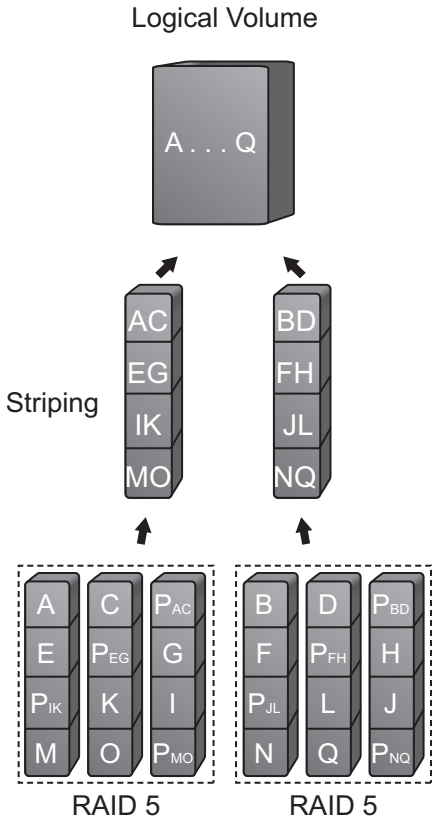


Figure A-8 RAID 50 disk array

A.10 RAID 60

RAID 60 arrays are formed by striping data across RAID 6 sub-arrays. Striping increases the system capacity and performance without adding disks to the array. It features dual parity, which allows for a possible failure of two disks in each array.

RAID 60: Striping with dual parity

Characteristics

- Storage capacity = [(number of disks in each subarray) -1] x (number of subarrays) x (capacity of the smallest disk)
- A minimum of eight disks are required.
- More fault tolerant than RAID 5
- Dual parity allows two disk failures in each array.
- Increased capacity and performance thanks to striping.

Recommended use

- Data archiving/ backing up
- High availability applications
- Large capacity servers

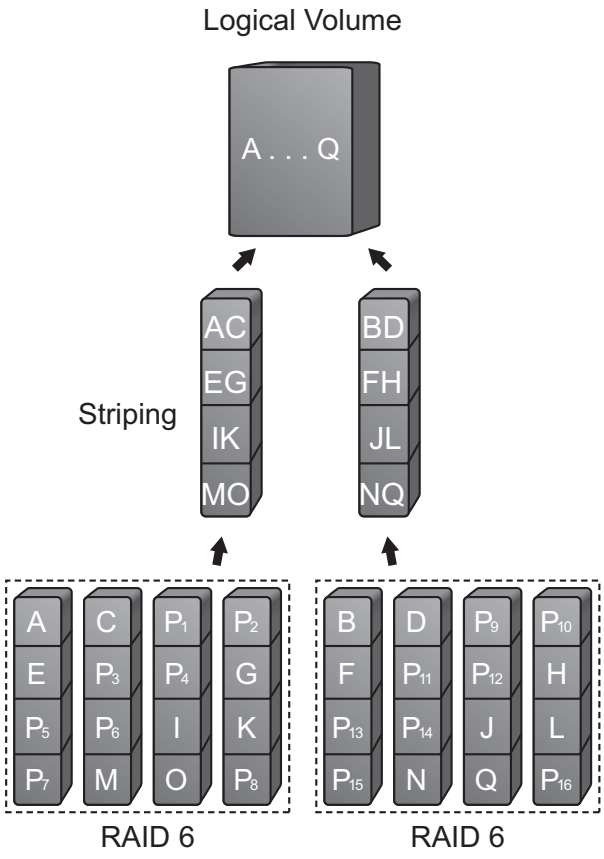


Figure A-9 RAID 60 disk array

A.11 JBOD

JBOD ("Just a Bunch of Disks") focuses on individual drives. The operating system sees each drive as an individual drive in JBOD mode. Therefore, the total capacity of JBOD is the sum of the capacities of each disk. This allows the user to add disks until the desired total capacity is reached. However, there is no RAID protection in this mode.

JBOD: Spanned disk array without fault tolerance

Characteristics

- Large capacity
- No fault tolerance

Recommended use

- Data backing up
- Large capacity servers

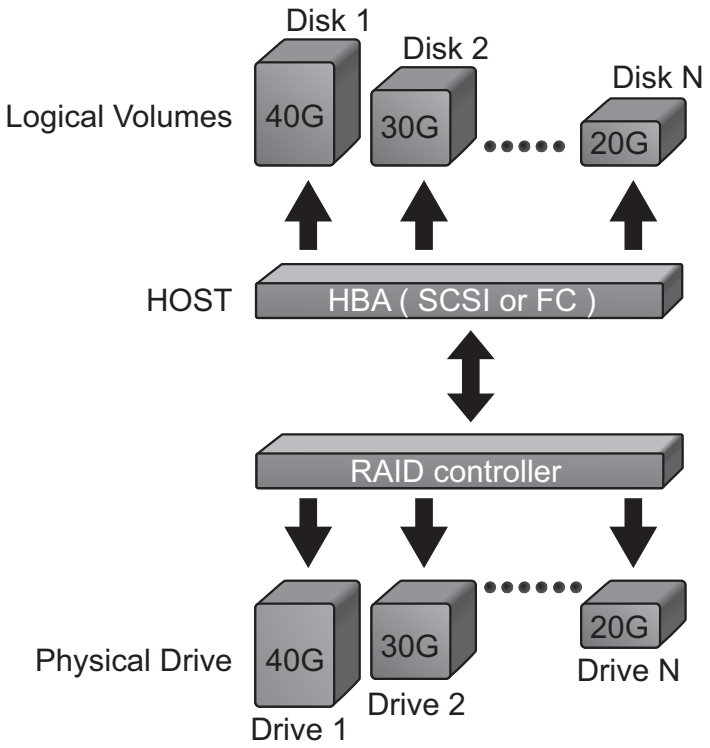


Figure A-10 JBOD disk array

A.12 NRAID

NRAID ("None RAID") combines all drives as one simple logical volume. The capacity of this volume is the total capacity of the physical member disks. NRAID does not have data redundancy.

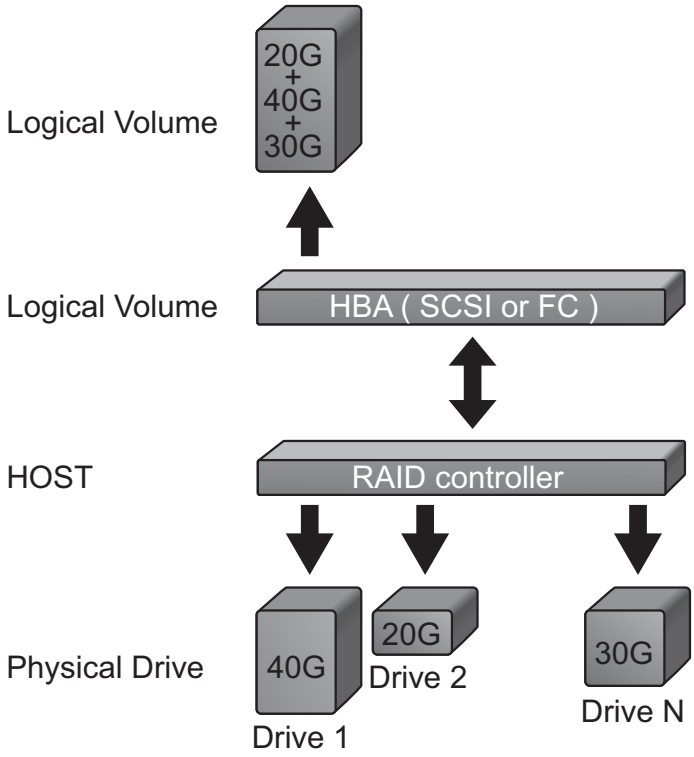


Figure A-11 NRAID

Appendix B: Features and Benefits

B.1 Overview

With the comprehensive features and utilities of the firmware, the system administrators can easily build solutions that meet business requirements as well as conduct management tasks effortlessly. The firmware offers not only performance and reliability but also capabilities to effectively maximize storage resources. It is a well-balanced mix of powerful functionalities and user-friendly management interfaces. The firmware is designed with the following twelve key features:

- Flexible storage presentation
- Flexible storage provisioning
- Comprehensive RAID configurations
- Dynamic configuration migration
- Effective capacity management
- Adaptive performance optimization
- Proactive data protection
- Fortified reliability and robustness
- Vigilant system monitoring
- Convenient task management
- Extensive supportive tools
- Easy-to-use user interfaces

B.2 Flexible Storage Presentation

Storage presentation refers to the process to export internal storage resources to be used by the host computers. As a storage system may be deployed in different environments or even shared by different types of host computers at the same time, the RAID controller firmware offers flexible storage presentation to accommodate these different requirements in order to accomplish effective storage sharing and minimize the management efforts.

- **Flexible storage presentation**

To simplify the storage presentation for different environments, the firmware provides the following presentation methods:

Simple presentation for direct attached storage (DAS) environment

Symmetric presentation for host computers with multiple IO path (MPIO) software

Selective presentation for sophisticated storage area network (SAN) environments

The administrators can choose an appropriate presentation method according to the environment to quickly complete the presentation at the deployment stage and effectively manage the presentation at the maintenance stage.

- **Host and LUN management**

The host HBA ports are managed by groups and the internal storage resources are exported as LUNs managed in distinct storage groups. Because the storage presentation can be conducted based on the groups, the presentation process can be simplified and more easily managed.

- **Independent LUN attributes**

Each LUN can have different attributes, such as CHS geometry, sector size, and optimization policy. All LUNs can be independently and dynamically masked or unmasked. IO access control of LUN can be also enforced for security or for isolating problematic host computers. Because each LUN can be independently configured, storage resources can be virtualized and shared without unnecessary compromise.

B.3 Flexible Storage Provisioning

Storage provisioning is the process to organize the physical disks with appropriate RAID configurations, which determine the level of performance and reliability of LUNs. The more RAID configurations a storage system can provide the more types of applications that the system can serve. The RAID controller firmware supports versatile RAID configurations as well as flexible storage provisioning that can achieve high utilization of disk space and enable sharing storage resources.

- **Comprehensive RAID configurations**

To fulfill different requirements, a variety of RAID configurations are offered:

Multiple disk groups (multiple array)

Multiple logical disks per disk group (support RAID partitioning)

Variable RAID levels supported

Variable stripe sizes supported

Hot spare with both global spare and local spare

Support auto-spare option for data rebuilding on unused disks

- **Multiple RAID configurations on single disk group**

Contrary to legacy RAID partitioning, by which all logical disks are merely partitions of a disk group and they have the same RAID configurations, the firmware offers flexible storage presentation, where multiple RAID levels and

stripe sizes can coexist in single disk group. This largely improves the utilization of disk space as well as simplifies the configuration planning.

- **Online volume management**

The firmware provides online volume management to build LUNs of multi-level RAID by striping over two or more logical disks for higher performance (aggregating horsepower of more disks), better reliability (multiple independent parity), and larger capacity (distributing data over more disks). To further utilize the disk space, a capacity-oriented volume can be created by concatenating multiple logical disks of different capacity to form storage with huge capacity. Without the embedded volume management, the administrator is required to use different host-based volume management software for different operating systems, which results in difficulties in managing volume configurations and risks of configuration lost if there is anything wrong with the host computers.

- **RAID quick setup**

Within very few steps, the administrator can complete the RAID configurations for all disks as well as basic system settings. The RAID quick setup is provided through multiple user interfaces: Web GUI, CLI, and LCD. By the RAID quick setup, a reliable storage system can quickly be available within only a few minutes, needing no sophisticated expertise.

B.4 Comprehensive RAID Configurations

RAID (Redundant Array of Independent Disks) technologies are deemed as the most promising solutions for building disk-based massive storage systems with high performance and reliability. The RAID controller firmware provides comprehensive RAID levels and stripe sizes such that a storage system can fulfill different types of requirements. In addition, valuable enhancements are also provided to offer useful flexibilities. Combining with flexible storage provisioning and presentation, the firmware can unleash the power of the controller and meet users' needs.

- **Comprehensive RAID levels**

The firmware supports a variety of RAID levels: RAID 0, 1, 3, 5, 6, 10, 30, 50, 60, NAND, and JBOD. You may freely choose the RAID levels that fit your applications well with a balanced set of performance, capacity, and reliability.

- **Selective stripe sizes**

The firmware supports stripe sizes of 4KB, 8KB, 16KB, 32KB, 64KB, 128KB, 256KB, and 512KB. To serve small-sized access, smaller stripe sizes are advised to shorten the response time and increase the number of accesses processed. On the other hand, for bulky-data access, bigger stripe sizes are advised to improve the throughput.

- **Selective initialization method and mode**

To initialize a logical disk, either data zeroing or background parity regeneration can be used. The administrator can choose to execute the background initialization for all logical disks simultaneously or one by one sequentially. To avoid confusing the operating systems, the background initialization will also clean up the data on the first few sectors to erase the file system super blocks. To speed up the initialization, the administrator can also choose to initialize the disk group and skip the initialization of logical disks.

- **Selective rebuild mode**

The rebuild mode of a disk group determines the rebuilding order of logical disks on the disk group. Three rebuild modes are available: parallel, sequential, and prioritized, by which the rebuilding will be done simultaneously for all logical disks, sequentially from the first to the last logical disks, and sequentially according to the order specified by the administrator, respectively.

- **Flexible hot spare policy**

Hot spare disks are standby disks that are used for replacing faulty disks by rebuilding the data of the faulty disks. Spare disks can be configured as local spare dedicated to specific disk group or global spare shared by all disk groups. Users can also enable the auto-spare option to force the spare disk returns to standby after the faulty disks are replaced by newer disks. This helps to control the physical organization of hard disks in the chassis.

B.5 Dynamic Configuration Migration

Business and users' needs are dynamic, and the storage systems are required to be aligned dynamically with the business requirements. As a result, the administrators need to reconfigure the storage from time to time. The RAID controllers are equipped with extensive utilities for online migration of the RAID configurations while retaining the system availability. Without the online reconfiguration utilities, unwanted system downtime and efforts for offline manual reconfiguration will stop the administrator from optimizing the storage.

- **Online disk group expansion**

Expanding a disk group by adding hard disks to be its member disks enlarges the usable capacity of a disk group, and more logical disks can be created from the disk group. An administrator can start a disk group with few hard disks and expand the disk group later if more capacity is needed. The initial cost from disk purchase can be minimized while future expansion is guaranteed.

- **Online RAID level and stripe size migration**

For performance tuning or adjusting the reliability level, the RAID level and stripe size needs to be changed. To execute the online migration, the

controller will start a background task to perform the data re-layout operations; during the migration, RAID operations are still available to protect data and serve requests from host computers. Unlike other implementations where only specific RAID levels or stripe sizes can be migrated, the RAID controller firmware can do the migration virtually from all RAID levels and stripe sizes to others as long as the disk space is sufficient.

- **Simultaneous migration and expansion**

The RAID level migration, stripe size migration, and disk group expansion can be done simultaneously without adding extra overheads. This significantly reduces the reconfiguration efforts and time when multiple reconfigurations are needed.

- **Rebuild during RAID reconfiguration**

When a disk fails during the RAID reconfiguration, the reconfiguration will be paused and disk rebuilding will be started immediately. After the rebuilding is done, the reconfiguration will be resumed. Without rebuilding during reconfiguration, the reconfiguration is executed on the degraded disk group, and it will take longer time to complete the reconfiguration because large part of the data needs to be regenerated. The degradation period will be also longer, which means bad performance and higher probability of RAID crash. It is highly advised that the administrator should ask for rebuild disk during reconfiguration when online RAID reconfiguration is needed.

B.6 Effective Capacity Management

The spending on storage resources is rising faster than overall IT expenses, but there are still out-of-capacity emergencies. The space of some LUNs might be used up, while there are other LUNs with idle space. The RAID controller firmware allows the administrator to online resize the LUN capacity and easily manage the free space. Therefore, neither sophisticated resource planning nor tedious process to do data copy and LUN re-initialization is required. The storage resources can thus be effectively and flexibly utilized during all the life time.

- **Support expansion chassis attachment**

The controller is equipped with an expansion port for attaching expansion chassis. This helps to build a huge-capacity storage solution at lower cost than to purchase multiple RAID systems. The expansion port also offers a future-proof solution for capacity expansion that helps users to add more disk drives to a RAID system without adding switches or host bus adapters.

- **Online logical disk capacity expansion and shrink**

The capacity of a logical disk can be online expanded if there is free space on its disk group. The capacity is expanded by allocating adjacent free chunks and by relocating logical disks on the same disk group. The capacity can also be shrunk to release free space on a disk group. During the

capacity change, RAID operations are still available to protect data and serve requests from host computers.

- **Concurrent logical disk capacity and disk group expansion**

The logical disk capacity expansion can also be done simultaneously with disk group expansion, and as a result, users can expand the capacity of a LUN by adding more drives to its disk group. Without logical disk capacity expansion, the administrator is forced to create a new LUN after the disk group expansion is done. To use the capacity on the new LUN, either extra data management efforts like file system or application reconfiguration are needed, or the administrator needs to deploy volume management software on the host computer, which leads to extra cost, complexity, and efforts.

- **Autonomous free space management**

The free space on a disk group is managed as free chunks. A free chunk is created when an administrator deletes a logical disk or shrinks its capacity. Free chunks are for creating new logical disks or for expanding a logical disk. By visualizing the free space with easy management utilities, an administrator can easily manage the free space and avoid waste.

- **Online de-fragmentation**

To have a continuous free space for new logical disks, discontinuous free chunks on a disk group can be consolidated into one big free chunk. This is accomplished by a background task to move the data on the disk group. Without the online de-fragmentation, the administrator needs to manually move the data of logical disks, and unacceptable system downtime is thus introduced.

- **Online volume expansion and shrink**

The capacity of a volume can be online expanded by adding the logical disks to the volume, which concatenates the space of each logical disk to form a larger capacity. Because the expansion is done instantly without incurring any background tasks, users can quickly start using the added capacity without waiting. Users can also reduce the capacity of a volume by removing the concatenated logical disks. Freely expanding and shrinking a volume enables efficient storage resource management.

B.7 Adaptive Performance Optimization

The performance is one of the most important values of a storage system, because higher performance means the capability to support larger organization, more transactions, and higher productivity. The RAID controller firmware fully utilizes the state-of-art storage hardware technologies to deliver the best-of-breed performance. The administrator can further enhance the performance by setting the extensive configurable performance parameters offered by the firmware and monitor the performance regularly. The firmware also provides adaptive optimization

algorithms that can intelligently self-monitor and self-adjust the performance parameters.

- **Adaptive read-ahead (pre-read, pre-fetch) optimization**

Read-ahead operation improves the performance of sequential reads by pre-fetching data from disk drives according to current hosts' read commands. The firmware can further identify multiple sequential read streams in random access and perform pre-read for the streams. The administrator can also specify the pre-read depth for dynamical tuning.

- **Configurable write caching policies**

Write cache can improve the response time and concurrency level of hosts' write commands. With the write cache, the controller can merge consecutive write commands to single write command and lower the disk drive's utilization by avoiding over-write commands. On the other hand, to ensure the best data reliability, the write policy can be set as write-through to make sure all data is written to the disk media.

- **Performance monitoring**

The controller keeps extensive IO statistics for performance monitoring. The statistics include physical components, like host ports and disk drives, as well as logical objects, like LUN, cache, and logical disks. The complete picture of the storage performance profile is presented and performance tuning can be conducted more effectively.

- **Intelligent IO processing**

Intelligent IO processing algorithms are efficiently executed to optimize the command execution and streamline the data flow. Disk IO scheduler is deployed to reduce the number of disk access and minimize the seek time among disk access. Elaborated RAID algorithms are performed to minimize the number of parity update and shorten the response time. The administrator is allowed to control these optimizations and tune the corresponding parameters.

- **One-click performance optimization**

To free the administrators from understanding those sophisticated performance parameters and tedious performance tuning, the firmware provides predefined performance profiles for optimizing the storage system according to different workload. Simply by one click on the GUI, a storage system optimized for time-critical, transaction-oriented, or high-throughput applications can be built.

B.8 Proactive Data Protection

The most fundamental requirement for a storage system is to protect the data from all kinds of failures. The RAID controller firmware supports versatile RAID configurations for different levels of reliability requirement, including RAID 6 to tolerate double-drive failure, and Triple Parity for extreme data availability. It provides online utilities for proactive data protection to monitor disk health, minimize the risk of data loss, and avoid RAID degradation. RAID configurations can be recovered and imported even the RAID is corrupted.

- **Online disk scrubbing**

Bad sectors of a hard disk can be detected only when they are accessed, so bad sectors may stay a long time undetected if disk access pattern is unevenly distributed and the sectors reside on seldom-accessed areas. In disk rebuilding, all data on the surviving hard disks is needed to regenerate the data of the failed disk, and if there are bad sectors on the surviving disks, the data cannot be regenerated and gone forever. As the number of sectors per disk increases, this will be a very common issue to any disk-based storage systems. The firmware provides online disk scrubbing utility to test the entire disk surface by a background task and recover any bad sectors detected.

- **Online parity consistency check and recovery**

The ability to protect data in parity-based RAID relies on the correctness of parity information. There are certain conditions that the parity consistency might be corrupted, such as internal errors of hard drives or abnormal power-off of system while the cache of hard drives is enabled. To ensure higher data reliability, the administrator can instruct the controller to conduct parity check and recovery during disk scrubbing.

- **S.M.A.R.T. drive health monitoring and self-test**

S.M.A.R.T. stands for Self-Monitoring Analysis Reporting Technology, by which a hard disk can continuously self-monitor its key components and collect statistics as indicators of its health conditions. The hard disks are periodically polled, and the controller will alert the administrator and start disk cloning when the disks report warnings. The firmware can also instruct the disk drives to execute device self-test routines embedded in the disk drives; this effectively helps the users to identify defective disk drives.

- **Online bad sector reallocation and recovery with over-threshold alert**

Hard disks are likely to have more and more bad sectors after they are in service. When host computers access bad sectors, the controller rebuilds data and responds to host. In addition to leveraging on-disk reserved space for bad block reallocation, the controller uses the reserved space on hard disks for reallocating data of bad sectors. If the number of bad sectors

increases over the threshold specified by the administrator, alerts will be sent to the administrator, and disk cloning will be started automatically.

- **Online SMART disk cloning**

When a hard disk fails in a disk group, RAID enters the degradation state, which means lower performance, higher risk of data loss or RAID corruption. When a hard disk is likely to become faulty or unhealthy, such as bad sectors of a physical disk increases over a threshold, or a disk reports SMART warning, the controller will online copy all data of the disk to a spare disk. Moreover, should the source disk fails during the cloning, controller will start rebuilding on the cloning disk, and the rebuilding will skip the sectors where the cloning has been done. The disk cloning has been approved as the most effective solutions to prevent RAID degradation.

- **Transaction log and auto parity recovery**

The capability to rebuild data of parity-based data protection relies on the consistency of parity and data. However, the consistency might not be retained because of improper system shutdown when there are uncompleted write commands. To maintain the consistency, the controller keeps logs of write commands in the NVRAM, and when the controller is restarted, the parity affected by the uncompleted writes will be automatically recovered.

- **Battery backup protection**

The controller delays the writes to disk drives and caches the data in the memory for performance optimization, but this also causes risk because the data in the cache will be gone forever if the system is not properly powered off. The battery backup module retains the data in the cache memory during abnormal power loss, and when the system is restarted, the data in the cache memory will be flushed to the disk drives. As the size of cache memory installed grows increasingly, the data loss could lead to unrecoverable disasters for applications.

B.9 Fortified Reliability and Robustness

The mission of a RAID controller is not only to protect user data from disk drive failure but also any hazards that might cause data loss or system downtime. Both hardware and firmware of RAID controller has incorporated advanced mechanisms to fortify the data reliability and to ensure the system robustness. These designs are derived from our field experiences of more than one decade in all kinds of real-world environments dealing with host computers, disk drives, and hardware components. One of the best parts in the design is that the administrator can use the online utilities provided by the firmware to solve his problems without calling the services from the vendors.

- **Seasoned redundancy design**

The storage system availability is achieved by the redundancy design to eliminate single point of failure. The controller is equipped with redundant flash chips with advanced algorithms for error checking and bad block reallocation in the firmware to protect the controller from defect flash blocks and ensure longer life time of the controller. The firmware stores two copies of RAID meta data as well as bad block reallocation map on disk drives to avoid any data or RAID loss resulted from bad sectors.

- **Support multi-path**

Supporting multi-path solutions at host side, such as Microsoft® MPIO, system continuity can be achieved because the storage system can tolerate failures on the IO path, such as host bus adapters, switches, or cables, by distributing IO over multiple IO paths. This also improves performance by the dynamic load balancing as well as simplifies the storage presentation process.

- **Support active-active redundant controller**

The controller supports dual active-active configuration to tolerate controller failure. The host IO access and background tasks of a failed controller can be online taken over by the survival controller. And when the failed controller is replaced by a new controller, the system will return to optimal operation by redistributing the host IO access and background tasks back to the original controller.

- **Support UPS monitoring**

The firmware can monitor the attached UPS by the SMART UPS protocol through the RS232 ports. When the AC power is gone, the firmware will conduct the graceful shutdown to avoid unwanted data loss. The administrator can also configure the UPS to determine the shutdown and restart policies.

- **Online array roaming**

When a storage system cannot be recovered in a short time, the best choice to put the data on disk drives back online is to conduct the array roaming, by which the disk drives can be installed in another storage system, and the RAID configurations are recovered instantly. Besides, the background tasks previously running on the disk drives are also resumed. With the online array roaming, the administrator can online install the disk drives one by one to the system, and import the disk groups later. This avoids disrupting the running storage system, and simplifies the roaming process.

- **Online array recovery**

There are chances of RAID crash resulted from the transient failure of multiple disk drives, and the disk drives can still be working after being re-powered. The drives might stall when its firmware is locked or be unstable as they are getting old. It could also be because of the abnormal

environmental conditions, like bad air conditioning or vibrations, or because of failures of hardware components, like connectors or cables. When any of these happens, the data and RAID configurations are gone forever for most storage systems. With the online array recovery, the firmware can online recognize and recover the RAID configurations stored on disk drives and get the data back as long as the disk drives can be running again.

B.10 Vigilant System Monitoring

After a storage system is installed and starts serving the applications, one of the most important jobs for the administrators is to monitor the system status. The hardware components in a storage system, like disk drives, fans, or power supply units, might become unhealthy or even dead, and the environment might also be out of control. The firmware vigilantly watches these hardware components and environment, and alerts the administrators timely. It may also intelligently conduct necessary countermeasures to recover from the degradation or mitigate the risks.

- **Remote monitoring by Web GUI**

The web GUI displays the picture of the hardware components of the storage system, and shows their corresponding status. The administrator can quickly get the overview of the system status and easily understand what components need to be serviced. Because the GUI can be remotely accessed by web browsers, the monitoring can be done virtually anywhere in the world.

- **Non-volatile event logging**

To help the administrators to track the history of all state changes, the firmware records the log of events on the NVRAM of the controller. Because the logs are recorded on the controller, there is no need of extra software to keep the records. The logs can also be downloaded to the administrator's desktop for further analysis or long-term database, and it can be saved as a human-readable text file or CSV file for spreadsheet applications.

- **Timely event notification**

In addition to the audible alarm on the controller to alert the administrators, the firmware can also send out event notification email and SNMP traps. To make sure that the events are delivered to the recipients, redundant servers are used to pass the events. The administrator can also manually generate test events to see how events are logged and alerts are sent.

- **Selective logging and notification**

The firmware records a wide range of events, from informative events, like user login or management operations to critical events, like power supply unit failure or RAID crash. To help find specific events in the log, the events are classified into different severity levels and types. The administrator can choose the severity levels of events to be recorded, and different event recipients can also be notified of events of different severity level.

B.11 Convenient Task Management

The RAID controllers are equipped with extensive utilities to support the system administrator to conduct maintenance tasks, which may be to fortify the RAID protection by disk scrubbing, to reconfigure RAID attributes by migrating RAID level or stripe size, or to expand LUN capacity. There are also other tasks like disk rebuilding or disk cloning that are started by the firmware automatically. These tasks are done in the background and possess more or less performance impact to applications accessing the storage system. To avoid the unwanted downgrade of service levels, the background tasks are required to be manageable and the administrator needs to have the flexibility to control the tasks.

- **Schedulable task execution**

The administrator can schedule the background tasks with appropriate parameters to be started at a specific point of time, which may be off-peak hours to avoid degrading the performance of the system. Without this function, the administrator might be forced to run the task during business hours, or they have to wait till the end of business hours so as to execute the tasks manually.

- **Periodical task execution**

Periodical schedule can be set for the maintenance tasks with appropriate parameters. This frees the administrator from keeping records of when the tasks have been done and when to run the tasks again.

- **Task execution logging and notification**

Logs of task execution are recorded in the non-volatile memory on the controller, so that the administrator can easily track the execution history of the tasks. The firmware also sends out notifications to inform the administrator about the current status of the tasks; As a result, the administrator can easily monitor the progress, just like they are with the storage systems.

- **Task progress monitoring and auto-resume**

The firmware regularly provides the progress report of task execution as well as estimates when the tasks will be completed. This helps the administrator to better plan the corresponding actions and manage the expectation of end users in the organization. The progress is recorded on the hard disks, and if the storage system is restarted, either normally or abnormally, the tasks will be automatically resumed at the point when the storage system is powered off.

- **Disk-rebuild priority over maintenance tasks**

There are chances that a disk might fail during the execution of maintenance tasks. To minimize the period of RAID degradation, the maintenance task will be aborted or paused, and disk rebuilding will be executed immediately. This reduces the risk of data loss and avoids

unwanted performance impact. When the rebuilding is done, the paused tasks will be automatically resumed.

- **Task priority control**

Executing the background tasks needs to occupy system resources, like CPU time, memory bandwidth, or access to disk drive. The administrator can choose the priority of the background tasks to speed up the task execution or to prevent the task from disturbing the host accesses. For more flexibility, the priority control is independently set for different types of background task.

B.12 Extensive Supportive Tools

In addition to the fundamental storage functions, the RAID controller firmware also provides extensive supportive tools that help the administrator to do a better job when managing the storage resources. These tools are aimed to offer full control to the storage devices so as to make the most of the storage system as well as to simplify the management tasks. Most of these features are derived from the feedback of our customers or users who are experts of storage and servers. They might not be considered when doing specification comparison, but the administrator will definitely discover their usefulness when doing the real-world jobs.

- **Object names and creation time**

Most of the major manageable logical objects, like disk groups, logical disks, or host groups, can be labeled with text as their names or memos. The administrator is then freed from memorizing those identifiers. The creation time is also recorded so that the administrator can easily trace the age of the objects.

- **Augmented RAID parameters**

In addition to frequently used RAID configurations, like RAID levels, the firmware provides also alignment offset and disk group size truncation. The former is to improve IO performance by shifting the starting LBA so as to align the data stripes with the data organization of file systems. And the later is to truncate the size of disk drives in a disk group such that disk drives of slightly smaller size can still be used.

- **Real time management with NTP**

The controller is equipped with real-time clock (RTC) chip, so that controller can record events or conduct scheduled maintenance tasks following the wall-clock time and calendar. The firmware also supports Network Time Protocol (NTP) to synchronize its date and time with an external time server. This ensures that all the IT equipments have common time base to act upon.

- **Configuration management**

The controller stores the configurations on either the disk drives or the NVRAM of the controller. The administrator can download the

configurations and save it as a file on his desktops, and he can restore the configurations later, if needed for system recovery or apply the configuration files to other systems. The configurations can also be saved to disk drives such that the configurations can be restored from the disk drives after the array roaming.

- **Hardware parameters**

Extensive user-configurable parameters are provided for configuring the system. The administrator can choose the speed of connections of disk drives or host for better compatibility, or he can choose to set policies for IO processing, like maximum number of retries, time-out value, SMART polling period, on-disk cache control, and so on. The firmware also provides extensive hardware statistics that help the administrator to know the system better and to conduct integration diagnostics more effectively.

- **Management network interface**

Using network to manage IT infrastructure and devices has been a common practices, so a storage system is required to be easily adopted in a network environment. The firmware supports a variety of network protocols: HTTP, TELNET, SSH, SSL, DHCP, NTP, DNS, SNMP, and SMTP such that the storage system can be easily managed.

B.13 Easy-To-Use User Interfaces

A storage system is valued not only by its functionalities but also how user-friendly it is. The storage systems with RAID controller have been marketed as the most easy-to-use storage solutions in the market for years. The firmware provides comprehensive features while keeps everything simple. The administrator can quickly understand each operation and unleash the functions of the system more effectively. The storage system vendors can also benefit from that because the efforts for educating users and supporting users to conduct maintenance tasks can be largely reduced, and the technical support staff can focus on high-level planning or cultivating new business.

- **Web-based GUI**

The administrator can enjoy the friendly GUI by pervasive web browsers without installing any software. Because the GUI is platform-independent, it eases the administration access to the storage systems and largely reduces the potential risk of software interoperability. The RAIDGuard also features online help, by which the administrator can learn the system more easily.

- **Command line interface (CLI)**

The command line interface provides shortcuts for power users who want to complete tasks by quickly entering a few lines of text commands. People at testing labs can build the test configurations in seconds, and there is virtually no effort to repeat the commands. IT staff can also leverage the command

line interface to deploy single configuration over multiple storage systems by replaying the CLI scripts predefined by the administrator.

- **Support LCD panel**

The LCD panel provides a quick overview of the system status as well as a simple way for setting basic configurations. It is very convenient for people who don't have or don't want to have the knowledge about the detailed operations of a storage system. The system operators, like the staff in a security control center, can also easily communicate with the administrators by reporting the messages shown on the LCD panel.

- **Remote management by Web, TELNET, and SSH**

The administrator can connect to multiple storage systems by the networks from one computer to remotely monitor the system status and execute management tasks. The GUI can be accessed by web browsers, and the CLI can be accessed by the console of TELNET or secure shell (SSH). As there are more and more chances that the administrators are asked to support the IT infrastructure of branch offices that might be far away, the capability to support remote management largely reduces the administration efforts.

- **Administration access control**

As data is very important asset, access to the storage system must be carefully guarded. The firmware offers control of the access to the storage system operations. Two levels of access are provided: administrator and user; the former has the full access to the storage system, while the later can only monitor the system status without the permission to change the configurations. The access control not only enforces the security but also avoids configuration inconsistency.

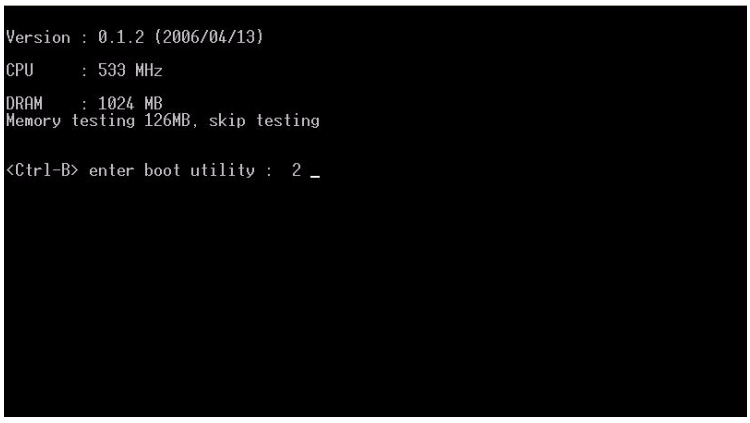
Appendix C: Boot Utility

Follow the steps below to enter the Boot Utility menu:

1. Run HyperTerminal (or the terminal program used to establish an RS232 connection with your RAID system) and open the connection established with your RAID system.

RS232 COM Port Setting	Bits per second: 115200
	Data bits: 8
	Parity: None
	Stop bits: 1
	Flow Control: None

2. Turn on the RAID system, the terminal shows the version, CPU and memory information.



3. You can press [ESC] to skip the memory test, and press [Ctrl+B] to enter the Boot Utility.

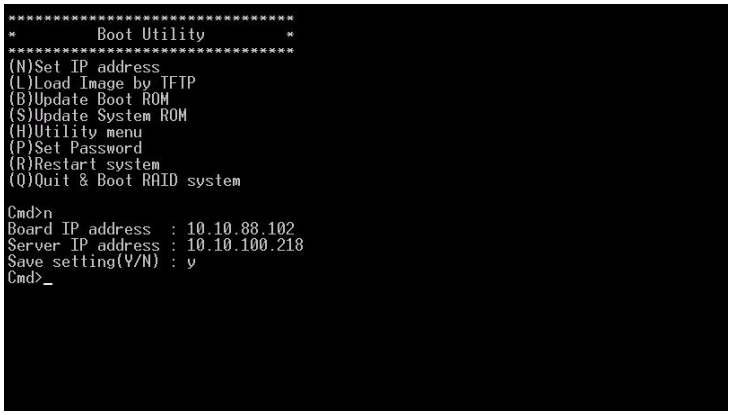
There are eight items in the Boot Utility menu.

(N) Set IP address	(H) Utility menu
(L) Load Image by TFTP	(P) Set Password
(B) Update Boot ROM	(R) Restart system
(S) Update System ROM	(Q) Quit & Boot RAID system

C.1 (N) Set IP address

The Boot Utility allows you to update the Boot ROM and System ROM. First you need to set the controller and server IP addresses. Press [N] to enter the settings.

1. Set the Board IP address and press [Enter].
2. Set the Server IP address and press [Enter].
3. Press [Y] to save the settings.



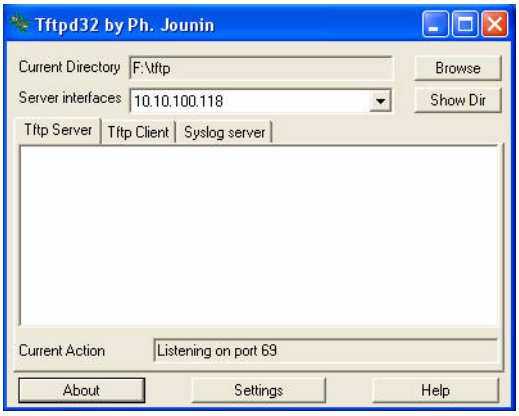
If your system supports redundant controller, press [N] and you are required to set the following IP addresses.

1. Set the Server IP address and press [Enter].
2. Set the Local IP address and press [Enter].
3. Set the Local IP mask address and press [Enter].
4. Set the Gateway address and press [Enter].

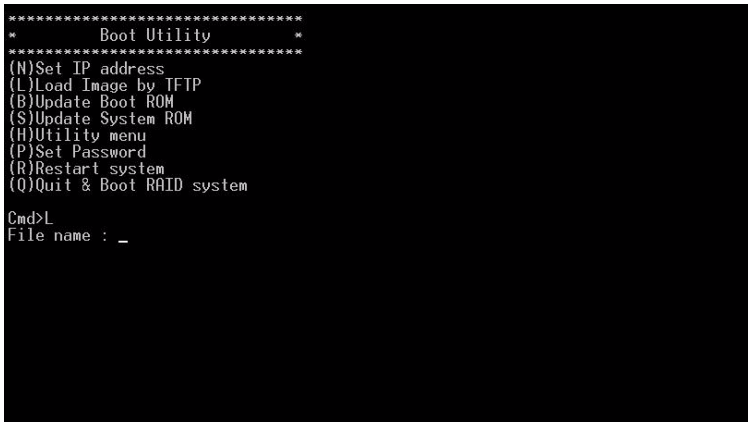
C.2 (L) Load Image by TFTP

Before a Boot ROM or System ROM update, you need to set up the TFTP server for loading a new firmware image. Follow the steps below to load an image:

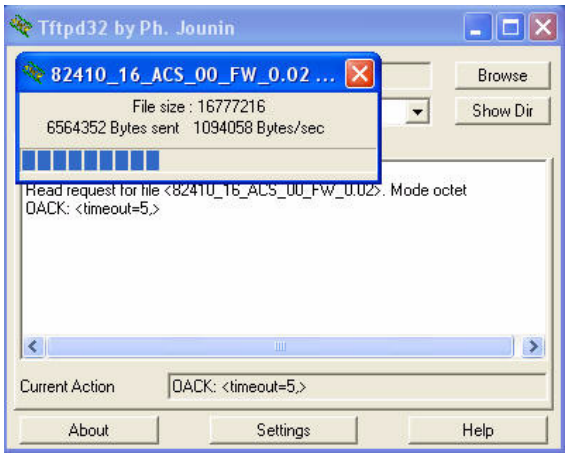
1. Open the TFTP Server, click the **Browse** button to set the boot code or firmware image directory. You can use the **Show Dir** button to see the files in the directory.



2. Press [L] in the Boot Utility and enter the file name of boot code of firmware.

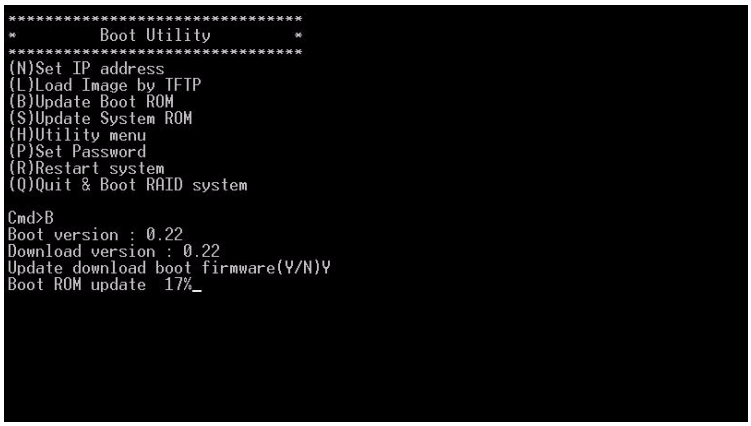


3. The TFTP server starts loading. When the loading is complete, you can proceed to update the Boot ROM or System ROM.



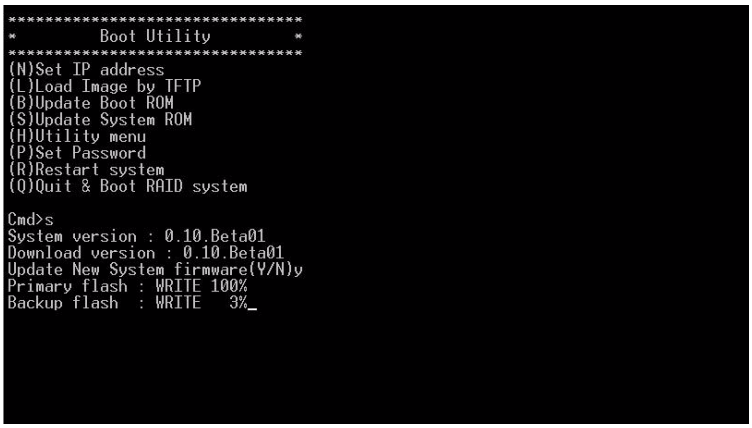
C.3 (B) Update Boot ROM

Press [B] to update the Boot ROM. The firmware versions and the **Update download boot firmware** message are displayed. Press [Y] to start the Boot ROM update. You can see the process percentage on the screen.



C.4 (S) Update System ROM

Press [S] to update the System ROM. The firmware versions and the **Update New System firmware** message are displayed. Press [Y] and the system starts to update the System ROM with the primary flash and backup flash. You can see the process percentages on the screen.



NOTE

Before a Boot ROM or System ROM update, make sure you have loaded the image by TFTP server. If not, the following message displays: **Invalid image size, load firmware first!**

C.5 (H) Utility menu

Press [H] to clear the Utility screen, and recall the Boot Utility menu.

C.6 (P) Set password

Press [P] to set or change the password for the Boot Utility login.

C.7 (R) Restart system

Press [R] to exit the Boot Utility and restart the RAID system.

C.8 (Q) Quit & Boot RAID system

Press [Q] to exit the Boot Utility, and the system starts to load the primary flash. When the loading is done, you can boot the RAID system.

Appendix D: Event Log Messages

D.1 RAID

- Disk operations

Event ID	0x0800				
Type	RAID	**Severity**	INFO	**Parameters**	Disk ID
Message	HDD**x** added				
Description	**hdd**x was added to the system from the user interface.				
Advice	None				

Event ID	0x0801				
Type	RAID	**Severity**	INFO	**Parameters**	Disk ID
Message	HDD**x** removed				
Description	**hdd**x was removed from the system from the user interface.				
Advice	None				

Event ID	0x0802				
Type	RAID	**Severity**	INFO	**Parameters**	Disk ID
Message	HDD**x** plugged				
Description	**hdd**x was added to the system by manual installation.				
Advice	None				

Event ID	0x0803				
Type	RAID	**Severity**	INFO	**Parameters**	Disk ID
Message	HDD**x** unplugged				
Description	**hdd**x was removed from the system by manual unplugging or **hdd**x failed to respond to the controller.				
Advice	None				

- Creation and deletion

Event ID	0x0c00				
Type	RAID	**Severity**	INFO	**Parameters**	JBOD ID
Message	JBOD**x** created				
Description	**jbd**x was created.				
Advice	None				

Event ID	0x0c01				
Type	RAID	**Severity**	INFO	**Parameters**	JBOD ID
Message	JBOD**x** deleted				
Description	**jbd**x was deleted.				
Advice	None				

Event ID	0x1000				
Type	RAID	**Severity**	INFO	**Parameters**	DG ID
Message	DG**x** created				
Description	**dg**x was created.				
Advice	None				

Event ID	0x1001				
Type	RAID	**Severity**	INFO	**Parameters**	DG ID
Message	DG**x** deleted				
Description	**dg**x was deleted.				
Advice	None				

Event ID	0x1800				
Type	RAID	**Severity**	INFO	**Parameters**	DG ID, LD ID
Message	DG**x**LD**y** created				
Description	**dg**x**ld**y was created.				
Advice	None				

Event ID	0x1801				
Type	RAID	**Severity**	INFO	**Parameters**	DG ID, LD ID
Message	DG**x**LD**y** deleted				
Description	**dg**x**ld**y was deleted.				
Advice	None				

Event ID	0x1c00				
Type	RAID	**Severity**	INFO	**Parameters**	VOL ID
Message	VOL**x** created				
Description	**vol**x was created.				
Advice	None				

Event ID	0x1c01				
Type	RAID	**Severity**	INFO	**Parameters**	VOL ID
Message	VOL**x** deleted				
Description	**vol**x was deleted.				
Advice	None				

- Initialization

Event ID	0x204c				
Type	RAID	**Severity**	INFO	**Parameters**	DG ID
Message	Write-zero init on DG**x** started				
Description	Disk group zeroing task on **dg**x was started.				
Advice	None				

Event ID	0x204d				
Type	RAID	**Severity**	INFO	**Parameters**	DG ID, LD ID
Message	Logical disk init on DG**x**LD**y** started				
Description	Logical disk initialization task on **dg**x**ld**y was started.				
Advice	None				

Event ID	0x204e				
Type	RAID	**Severity**	NOTICE	**Parameters**	DG ID
Message	Write-zero init on DG**x** completed				
Description	Disk group zeroing task on **dg**x was completed.				
Advice	None				

Event ID	0x204f				
Type	RAID	**Severity**	NOTICE	**Parameters**	DG ID, LD ID
Message	Logical disk init on DG**x**LD**y** completed				
Description	Logical disk initialization task on **dg**x was completed.				
Advice	None				

Event ID	0x2050				
Type	RAID	**Severity**	WARNING	**Parameters**	DG ID
Message	Write-zero init on DG**x** aborted				
Description	Disk group zeroing task on **dg**x was aborted.				
Advice	Check if any disks in the disk group failed, and then re-create the disk group.				

Event ID	0x2051				
Type	RAID	**Severity**	WARNING	**Parameters**	DG ID, LD ID
Message	Logical disk init on DG**x**LD**y** aborted				
Description	Logical disk initialization task on **dg**x**ld**y was aborted.				
Advice	Check if any disks in the disk group failed, and then re-create the logical disk.				

Event ID	0x2064				
Type	RAID	**Severity**	NOTICE	**Parameters**	Zeroing progress, DG ID, Notify threshold
Message	Write zero progress(**y**%) on DG**x** reach to the notify percent(**z**%)				
Description	The progress of zeroing DG has reached the notify threshold.				
Advice	None				

Event ID	0x2066				
Type	RAID	**Severity**	NOTICE	**Parameters**	Init progress, DG ID, LD ID, Notify threshold
Message	Logical disk init progress(**w**%) on DG**x**LD**y** reach the notify percent(**z**%)				
Description	The progress of initializing logical disk has reached the pre-define threshold.				
Advice	None				

- Spare

Event ID	0x0804				
Type	RAID	**Severity**	INFO	**Parameters**	Disk ID
Message	Global spare HDD**x** added				
Description	**hdd**x was selected to be a global spare.				
Advice	None				

Event ID	0x0805				
Type	RAID	**Severity**	INFO	**Parameters**	Disk ID
Message	Global spare HDD**x** removed				
Description	Global spare **hdd**x was changed to be an unused disk.				
Advice	None				

Event ID	0x1002				
Type	RAID	**Severity**	INFO	**Parameters**	Disk ID, DG ID
Message	Local spare HDD**x** of DG**y** added				
Description	**hdd**x was selected as local spare of **dg**y.				
Advice	None				

Event ID	0x1003				
Type	RAID	**Severity**	INFO	**Parameters**	Disk ID, DG ID
Message	Local spare HDD**x** of DG**y** removed				
Description	**dg**y's local spare, **hdd**x, was removed.				
Advice	None				

- Rebuild

Event ID	0x2000				
Type	RAID	**Severity**	NOTICE	**Parameters**	DG ID
Message	Rebuilding on DG**x** started				
Description	Disk rebuilding on **dg**x was started.				
Advice	None				

Event ID	0x2001				
Type	RAID	**Severity**	NOTICE	**Parameters**	DG ID
Message	Rebuilding on DG**x** completed				
Description	Disk rebuilding on **dg**x was completed.				
Advice	None				

Event ID	0x2002				
Type	RAID	**Severity**	WARNING	**Parameters**	DG ID
Message	Rebuilding on DG**x** aborted				
Description	Disk rebuilding on **dg**x was aborted.				
Advice	None				

Event ID	0x2063				
Type	RAID	**Severity**	NOTICE	**Parameters**	Rebuild progress, DG ID, Notify threshold
Message	Rebuild progress(**y**%) on DG**x** reach to the notify percent(**z**%)				
Description	The progress of rebuilding has reached the pre-define threshold.				
Advice	None				

- Roaming

Event ID	0x0820				
Type	RAID	**Severity**	INFO	**Parameters**	
Message	Disks changed during power-off				
Description	The number of disks installed is different when the controller was powered off. Either existing disks were removed or new disks were installed during power-off.				
Advice	Check hard disk status, and conduct roaming or recovery, if necessary.				

Event ID	0x1004				
Type	RAID	**Severity**	INFO	**Parameters**	DG ID
Message	DG**x** is imported				
Description	Foreign disk group has been imported to be **dg**x.				
Advice	None				

Event ID	0x1c02				
Type	RAID	**Severity**	INFO	**Parameters**	VOL ID
Message	VOL**x** is imported				
Description	Foreign volume has been imported to be **vol**x.				
Advice	None				

- Recovery

Event ID	0x2052				
Type	RAID	**Severity**	INFO	**Parameters**	DG ID
Message	DG**x** is recovered				
Description	Disk group **dg**x has been recovered.				
Advice	None				

Event ID	0x2053				
Type	RAID	**Severity**	INFO	**Parameters**	DG ID, LD ID
Message	DG**x**LD**y** is recovered				
Description	Logical disk **dg**x**ld**y has been recovered.				
Advice	None				

Event ID	0x2054				
Type	RAID	**Severity**	INFO	**Parameters**	VOL ID
Message	VOL**x** is recovered				
Description	Volume **vol**x has been recovered.				
Advice	None				

D.2 Task

- **Disk group expansion**

Event ID	0x2009				
Type	TASK	**Severity**	INFO	**Parameters**	DG ID
Message	Expansion on DG**x** started				
Description	Disk group expansion on **dg**x was started manually.				
Advice	None				

Event ID	0x202d				
Type	TASK	**Severity**	NOTICE	**Parameters**	DG ID
Message	Expansion on DG**x** started by schedule				
Description	Scheduled disk group expansion on **dg**x was started.				
Advice	None				

Event ID	0x2043				
Type	TASK	**Severity**	WARNING	**Parameters**	DG ID
Message	Expansion on DG**x** failed to start by schedule				
Description	Scheduled disk group expansion on **dg**x failed to start.				
Advice	Check if the disk group is busy or non-optimal when starting the task.				

Event ID	0x200c				
Type	TASK	**Severity**	NOTICE	**Parameters**	DG ID
Message	Expansion on DG**x** paused				
Description	Disk group expansion on **dg**x was paused.				
Advice	Check if there is failed member disk in the disk group during the task.				

Event ID	0x200d				
Type	TASK	**Severity**	NOTICE	**Parameters**	DG ID
Message	Expansion on DG**x** resumed				
Description	Disk group expansion on **dg**x was resumed.				
Advice	None				

Event ID	0x200a				
Type	TASK	**Severity**	NOTICE	**Parameters**	DG ID
Message	Expansion on DG**x** completed				
Description	Disk group expansion on **dg**x was completed.				
Advice	None				

Event ID	0x205f				
Type	TASK	**Severity**	NOTICE	**Parameters**	Expand progress, DG ID, Notify threshold
Message	DG expand progress(**y**%) on DG**x** reach to the notify percent(**z**%)				
Description	The progress of dg expanding has reached the pre-define thresh-old.				
Advice	None				

- Logical disk migration

Event ID	0x2004				
Type	TASK	**Severity**	INFO	**Parameters**	DG ID, LD ID
Message	Migration on DG**x**LD**y** started				
Description	Migration on **dg**x**ld**y was started manually.				
Advice	None				

Event ID	0x202c				
Type	TASK	**Severity**	NOTICE	**Parameters**	DG ID, LD ID
Message	Migration on DG**x**LD**y** started by schedule				
Description	Scheduled migration on **dg**x**ld**y was started.				
Advice	TBD				

Event ID	0x2044				
Type	TASK	**Severity**	WARNING	**Parameters**	DG ID, LD ID
Message	Migration on DG**x**LD**y** failed to start by schedule				
Description	Scheduled migration on **dg**x**ld**y failed to start.				
Advice	Check if the logical disk or the disk group is busy or non-optimal when starting the task.				

Event ID	0x2007				
Type	TASK	**Severity**	NOTICE	**Parameters**	DG ID, LD ID
Message	Migration on DG**x**LD**y** paused				
Description	Migration on **dg**x**ld**y was paused.				
Advice	Check if the logical disk or the disk group is non-optimal during the task.				

Event ID	0x2008				
Type	TASK	**Severity**	NOTICE	**Parameters**	DG ID, LD ID
Message	Migration on DG**x**LD**y** resumed				
Description	Migration on **dg**x**ld**y was resumed.				
Advice	None				

Event ID	0x2006				
Type	TASK	**Severity**	WARNING	**Parameters**	DG ID, LD ID
Message	Migration on DG**x**LD**y** aborted				
Description	Migration on **dg**x**ld**y was aborted.				
Advice	Check if the logical disk is faulty.				

Event ID	0x2005				
Type	TASK	**Severity**	NOTICE	**Parameters**	DG ID, LD ID
Message	Migration on DG**x**LD**y** completed				
Description	Migration on **dg**x**ld**y was completed.				
Advice	None				

Event ID	0x2061				
Type	TASK	**Severity**	NOTICE	**Parameters**	Migrate progress, DG ID, Notify threshold
Message	LD migrate progress(**y**%) on DG**x** reach to the notify percent(**z**%)				
Description	The progress of LD migration has reached the pre-define threshold.				
Advice	None				

Event ID	0x206e				
Type	TASK	Severity	NOTICE	Parameters	Migrate progress, DG ID, LD ID, Notify threshold
Message	LD migrate progress(**w**%) on DG**x**LD**y** reach to the notify percent(**z**%)				
Description	The progress of LD migration has reached the pre-define threshold.				
Advice	None				

- Logical disk capacity expansion

Event ID	0x2037				
Type	TASK	Severity	INFO	Parameters	DG ID, LD ID
Message	Expansion on DG**x**LD**y** started				
Description	Logical disk capacity expansion on **dg**x**ld**y was started manually.				
Advice	None				

Event ID	0x202e				
Type	TASK	Severity	NOTICE	Parameters	DG ID, LD ID
Message	Expansion on DG**x**LD**y** started by schedule				
Description	Scheduled logical disk capacity expansion on **dg**x**ld**y was started.				
Advice	None				

Event ID	0x2045				
Type	TASK	Severity	WARNING	Parameters	DG ID, LD ID
Message	Expansion on DG**x**LD**y** failed to start by schedule				
Description	Scheduled logical disk capacity expansion on **dg**x**ld**y failed to start.				
Advice	Check if the logical disk or the disk group is busy or non-optimal when starting the task.				

Event ID	0x2031				
Type	TASK	**Severity**	NOTICE	**Parameters**	DG ID, LD ID
Message	Expansion on DG**x**LD**y** paused				
Description	Logical disk capacity expansion on **dg**x**ld**y was paused.				
Advice	Check if a member disk in the disk group failed during the task.				

Event ID	0x2032				
Type	TASK	**Severity**	NOTICE	**Parameters**	DG ID, LD ID
Message	Expansion on DG**x**LD**y** resumed				
Description	Logical disk capacity expansion on **dg**x**ld**y was resumed.				
Advice	None				

Event ID	0x2030				
Type	TASK	**Severity**	WARNING	**Parameters**	DG ID, LD ID
Message	Expansion on DG**x**LD**y** aborted				
Description	Logical disk capacity expansion on **dg**x**ld**y was aborted.				
Advice	Check if the disk group is faulty during the task. (TBD)				

Event ID	0x202f				
Type	TASK	**Severity**	NOTICE	**Parameters**	DG ID, LD ID
Message	Expansion on DG**x**LD**y** completed				
Description	Logical disk capacity expansion on **dg**x**ld**y is complete.				
Advice	Hosts might need to rescan the LUN of the logical disk to get the updated capacity. The partitions or file systems on the logical disk has to be grown to access the newly created space.				

Event ID	0x2060				
Type	TASK	**Severity**	NOTICE	**Parameters**	Expand progress, DG ID, Notify threshold
Message	LD expand progress(**y**%) on DG**x** reach to the notify percent(**z**%)				
Description	The progress of LD expanding has reached the pre-define thresh-old.				
Advice	None				

- Logical disk shrink

Event ID	0x200e				
Type	TASK	**Severity**	NOTICE	**Parameters**	DG ID, LD ID
Message	DG**x**LD**y** shrinked				
Description	DG**x**LD**y** shrinked				
Advice	Make sure partitions or file systems on the logical disk have been shrunk before conducting the logical disk capacity shrink. After finishing, hosts might need to rescan the LUN of the logical disk to get the updated capacity.				

- Disk group defragmentation

Event ID	0x2010				
Type	TASK	**Severity**	INFO	**Parameters**	DG ID
Message	Defragment on DG**x** started				
Description	Disk group defragment on **dg**x was started manually.				
Advice	None				

Event ID	0x2033				
Type	TASK	**Severity**	NOTICE	**Parameters**	DG ID
Message	Defragment on DG**x** started by schedule				
Description	Scheduled disk group defragment on **dg**x was started.				
Advice	None				

Event ID	0x2047				
Type	TASK	**Severity**	WARNING	**Parameters**	DG ID
Message	Defragment on DG**x** failed to start by schedule				
Description	Scheduled disk group defragment on **dg**x failed to start.				
Advice	Check if the disk group is busy or non-optimal when starting the task.				

Event ID	0x2013				
Type	TASK	**Severity**	NOTICE	**Parameters**	DG ID
Message	Defragment on DG**x** paused				
Description	Disk group defragment on **dg**x was paused.				
Advice	Check if there is failed member disk in the disk group during the task.				

Event ID	0x2014				
Type	TASK	**Severity**	NOTICE	**Parameters**	DG ID
Message	Defragment on DG**x** resumed				
Description	Disk group defragment on **dg**x was resumed.				
Advice	None				

Event ID	0x2011				
Type	TASK	**Severity**	NOTICE	**Parameters**	DG ID
Message	Defragment on DG**x** completed				
Description	Disk group defragment on **dg**x was completed.				
Advice	None				

Event ID	0x205e				
Type	TASK	**Severity**	NOTICE	**Parameters**	Defrag progress, DG ID, Notify threshold
Message	Defrag progress(**y**%) on DG**x** reach to the notify percent(**z**%)				
Description	The progress of defragmentation has reached the pre-define threshold.				
Advice	None				

- Volume expansion

Event ID	0x202a				
Type	TASK	**Severity**	NOTICE	**Parameters**	VOL ID
Message	VOL**x** expanded				
Description	Volume capacity expansion on **vol**x was completed.				
Advice	Hosts might need to rescan the LUN of the volume to get the updated capacity, and the partitions or file systems on the volume has to be grown to access the newly created space.				

- Disk cloning

Event ID	0x2015				
Type	TASK	**Severity**	INFO	**Parameters**	DISK ID, DISK ID
Message	Clone from HDD**x** to HDD**y** started				
Description	Disk cloning from **hdd**x to **hdd**y was started manually.				
Advice	None				

Event ID	0x2034				
Type	TASK	**Severity**	NOTICE	**Parameters**	DISK ID, DISK ID
Message	Clone from HDD**x** to HDD**y** auto started				
Description	Disk cloning from **hdd**x to **hdd**y was started by SMART warning, BBR-over-threshold event, or by schedule.				
Advice	None				

Event ID	0x2048				
Type	TASK	**Severity**	WARNING	**Parameters**	DISK ID, DISK ID
Message	Clone from HDD**x** to HDD**y** failed to auto start				
Description	Auto disk cloning from **hdd**x to **hdd**y failed to start.				
Advice	Check if the disk failed or the source disk group is non-optimal when starting the task.				

Event ID	0x2018				
Type	TASK	**Severity**	NOTICE	**Parameters**	DISK ID, DISK ID
Message	Clone from HDD**x** to HDD**y** paused				
Description	Disk cloning from **hdd**x to **hdd**y was paused.				
Advice	Check if the source disk group is busy or non-optimal during the task.				

Event ID	0x2019				
Type	TASK	**Severity**	NOTICE	**Parameters**	DISK ID, DISK ID
Message	Clone from HDD**x** to HDD**y** resumed				
Description	Disk cloning from **hdd**x to **hdd**y was resumed.				
Advice	None				

Event ID	0x2017				
Type	TASK	**Severity**	INFO	**Parameters**	DISK ID, DISK ID
Message	Clone from HDD**x** to HDD**y** stopped				
Description	Disk cloning from **hdd**x to **hdd**y was stopped manually.				
Advice	None				

Event ID	0x201a				
Type	TASK	**Severity**	WARNING	**Parameters**	DISK ID, DISK ID
Message	Clone from HDD**x** to HDD**y** aborted				
Description	Clone from **hdd**x to **hdd**y was aborted.				
Advice	Check if the disk failed or the target disk was rebuilding when the source disk failed.				

Event ID	0x2016				
Type	TASK	**Severity**	NOTICE	**Parameters**	DISK ID, DISK ID
Message	Clone from HDD**x** to HDD**y** completed				
Description	Disk cloning from **hdd**x to **hdd**y is complete.				
Advice	None				

Event ID	0x2056				
Type	TASK	**Severity**	NOTICE	**Parameters**	DISK ID, DISK ID
Message	Clone from HDD**x** to HDD**y** auto-resumed				
Description	Disk cloning from **hdd**x to **hdd**y was auto-resumed.				
Advice	None				

Event ID	0x206f				
Type	TASK	**Severity**	NOTICE	**Parameters**	Clone progress, DISK ID, DISK ID, Notify threshold
Message	Clone progress(**w**%) from HDD**x** to HDD**y** reach to the notify percent(**z**%)				
Description	The progress of disk cloning has reached the pre-define threshold.				
Advice	None				

- Disk scrubbing of hard disks

Event ID	0x201c				
Type	TASK	**Severity**	INFO	**Parameters**	DISK ID
Message	Scrub on HDD**x** started				
Description	Disk scrubbing on **hdd**x was started manually.				
Advice	None				

Event ID	0x2035				
Type	TASK	**Severity**	NOTICE	**Parameters**	DISK ID
Message	Scrub on HDD**x** started by schedule				
Description	Scheduled disk scrubbing on **hdd**x was started.				
Advice	None				

Event ID	0x204a				
Type	TASK	**Severity**	WARNING	**Parameters**	DISK ID
Message	Scrub on HDD**x** failed to start by schedule				
Description	Scheduled disk scrubbing on **hdd**x failed to start.				
Advice	Check if the disk is off-line or busy.				

Event ID	0x2020				
Type	TASK	**Severity**	INFO	**Parameters**	DISK ID, Sector Num
Message	Scrub on HDD**x** stopped with **y** bad sectors detected				
Description	Disk scrubbing on **hdd**x was stopped manually, and **y** bad sectors were detected.				
Advice	If the number of bad sectors grows exceptionally fast or beyond a reasonable number, consider to conduct diagnostics and replace with new disks.				

Event ID	0x2055				
Type	TASK	**Severity**	WARNING	**Parameters**	DISK ID, Sector Num
Message	Scrub on HDD**x** aborted with **y** bad sectors detected				
Description	Disk scrubbing on **hdd**x was aborted, and **y** bad sectors were				
Advice	Check if the disk is off-line or busy.				

Event ID	0x2038				
Type	TASK	**Severity**	NOTICE	**Parameters**	DISK ID, Sector Num
Message	Scrub on HDD**x** completed with **y** bad sectors detected				
Description	Disk scrubbing on **hdd**x was completed, and **y** bad sectors were				
Advice	If the number of bad sectors grows exceptionally fast or beyond a reasonable number, consider conducting diagnostics and replace with new disks.				

Event ID	0x2065				
Type	TASK	**Severity**	NOTICE	**Parameters**	Scrub. Progress, DISK ID, Notify threshold
Message	Scrub progress(**y**%) on HDD**x** reach to the notify percent(**z**%)				
Description	The progress of scrubbing disk has reached the pre-define threshold.				
Advice	None				

- Disk scrubbing of disk groups

Event ID	0x201d				
Type	TASK	**Severity**	INFO	**Parameters**	DG ID
Message	Scrub on DG**x** started				
Description	Disk scrubbing on **dg**x was started manually.				
Advice	None				

Event ID	0x2036				
Type	TASK	**Severity**	NOTICE	**Parameters**	DG ID
Message	Scrub on DG**x** started by schedule				
Description	Scheduled disk scrubbing on **dg**x was started.				
Advice	None				

Event ID	0x2049				
Type	TASK	**Severity**	WARNING	**Parameters**	DG ID
Message	Scrub on DG**x** failed to start by schedule				
Description	Scheduled disk scrubbing on **dg**x failed to start.				
Advice	Check if the disk group is busy or non-optimal.				

Event ID	0x2021				
Type	TASK	**Severity**	INFO	**Parameters**	DG ID, Sector Num, Row Num, Row Num
Message	Scrub on DG**w** stopped with **x** bad sectors detected, **y** inconsistent rows found, and **z** rows recovered				
Description	Disk scrubbing on **dg**w was stopped manually, and there were **x** bad sectors detected, **y** inconsistent rows found, and **z** rows recovered.				
Advice	If the number of bad sectors or inconsistent rows grows exceptionally fast or beyond a reasonable number, consider to conduct diagnostics and replace with new disks.				

Event ID	0x2023				
Type	TASK	**Severity**	NOTICE	**Parameters**	DG ID, Sector Num, Row Num, Row Num
Message	Scrub on DG**w** aborted with **x** bad sectors detected, **y** inconsistent rows found, and **z** rows recovered				
Description	Disk scrubbing on **dg**w was aborted, and there were **x** bad sectors detected, **y** inconsistent rows found, and **z** rows recovered.				
Advice	Check if the disk group is busy or non-optimal.				

Event ID	0x2039				
Type	TASK	**Severity**	NOTICE	**Parameters**	DISK ID, Sector Num, Row Num, Row Num
Message	Scrub on DG**w** completed with **x** bad sectors detected, **y** inconsistent rows found, and **z** rows recovered				
Description	Disk scrubbing on **dg**w was completed, and there were **x** bad sectors detected, **y** inconsistent rows found, and **z** rows recovered.				
Advice	If the number of bad sectors grows exceptionally fast or beyond a reasonable number, consider to conduct diagnostics and replace with new disks.				

Event ID	0x205d				
Type	TASK	**Severity**	NOTICE	**Parameters**	Scrub. Progress, DG ID, Notify threshold
Message	Scrub progress(**y**%) on DG**x** reach to the notify percent(**z**%)				
Description	The progress of scrubbing on **dg**x has reached the pre-define threshold.				
Advice	None				

NOTE:

Because one disk group can have only one logical disk executing disk scrubbing, the events do not record ID of the logical disk to execute disk scrubbing.

- **Disk scrubbing of logic disks**

Event ID	0x2040				
Type	TASK	**Severity**	INFO	**Parameters**	DG ID, LD_ID
Message	Scrub on DG**x**LD**y** started				
Description	Disk scrubbing on **dg**x**ld**y was started manually.				
Advice	None				

Event ID	0x204b				
Type	TASK	**Severity**	NOTICE	**Parameters**	DG ID, LD_ID
Message	Scrub on DG**x**LD**y** started by schedule				
Description	Scheduled disk scrubbing on **dg**x was started.				
Advice	None				

Event ID	0x2057				
Type	TASK	**Severity**	WARNING	**Parameters**	DG ID, LD_ID
Message	Scrub on DG**x**LD**y** failed to start by schedule				
Description	Scheduled disk scrubbing on **dg**x**ld**y failed to start.				
Advice	Check if the logic disk is busy or non-optimal.				

Event ID	0x2041				
Type	TASK	**Severity**	INFO	**Parameters**	DG ID, LD_ID, Sector Num, Row Num, Row Num
Message	Scrub on DG**v**LD**w** stopped with **x** bad sectors detected, **y** inconsistent rows found, and **z** rows recovered				
Description	Disk scrubbing on **dg**v**ld**w was stopped manually, and there were **x** bad sectors detected, **y** inconsistent rows found, and **z** rows recovered.				
Advice	If the number of bad sectors or inconsistent rows grows exceptionally fast or beyond a reasonable number, consider to conduct diagnostics and replace with new disks.				

Event ID	0x2042				
Type	TASK	**Severity**	NOTICE	**Parameters**	DG ID, LD_ID, Sector Num, Row Num, Row Num
Message	Scrub on DG**v**LD**w** aborted with **x** bad sectors detected, **y** inconsistent rows found, and **z** rows recovered				
Description	Disk scrubbing on **dg**v**ld**w was aborted, and there were **x** bad sectors detected, **y** inconsistent rows found, and **z** rows recovered.				
Advice	Check if the logical disk is busy or non-optimal.				

Event ID	0x203a				
Type	TASK	**Severity**	NOTICE	**Parameters**	DG ID, LD_ID, Sector Num, Row Num, Row Num
Message	Scrub on DG**v**LD**w** completed with **x** bad sectors detected, **y** inconsistent rows found, and **z** rows recovered				
Description	Disk scrubbing on **dg**v**ld**w was completed, and there were **x** bad sectors detected, **y** inconsistent rows found, and **z** rows recovered.				
Advice	If the number of bad sectors grows exceptionally fast or beyond a reasonable number, consider to conduct diagnostics and replace with new disks.				

Event ID	0x206d				
Type	TASK	**Severity**	NOTICE	**Parameters**	Scrub. Progress, DG ID, LD_ID, Notify threshold
Message	Scrub progress(**w**%) on DG**x**LD**y** reach to the notify percent(**z**%)				
Description	The progress of scrubbing on **dg**x**ld**y has reached the pre-define threshold.				
Advice	None				

- Disk group parity regeneration

Event ID	0x2024				
Type	TASK	**Severity**	INFO	**Parameters**	DG ID
Message	Reg. parity on DG**x** started				
Description	Reg. parity on **dg**x was started manually.				
Advice	None				

Event ID	0x2026				
Type	TASK	**Severity**	WARNING	**Parameters**	DG ID
Message	Reg. parity on DG**x** aborted				
Description	Reg. parity on **dg**x was aborted.				
Advice	Check if the disk group is busy or non-optimal.				

Event ID	0x2027				
Type	TASK	**Severity**	INFO	**Parameters**	DG ID
Message	Reg. parity on DG**x** stopped				
Description	Reg. parity on **dg**x was stopped manually.				
Advice	None				

Event ID	0x2025				
Type	TASK	**Severity**	NOTICE	**Parameters**	DG ID
Message	Reg. parity on DG**x** completed				
Description	Reg. parity on **dg**x was completed.				
Advice	None				

Event ID	0x205c				
Type	TASK	**Severity**	NOTICE	**Parameters**	Reg. Prog-ress, DG ID, Notify threshold
Message	Reg. progress(**y**%) on DG**x** reach to the notify percent(**z**%)				
Description	The progress of Reg. parity on **dg**x has reached the pre-define threshold.				
Advice	None				

- Logic disk parity regeneration

Event ID	0x203c				
Type	TASK	**Severity**	INFO	**Parameters**	DG ID, LD_ID
Message	Reg. parity on DG**x**LD**y** started				
Description	Reg. parity on **dg**x**ld**y was started manually.				
Advice	None				

Event ID	0x203e				
Type	TASK	**Severity**	WARNING	**Parameters**	DG ID, LD_ID
Message	Reg. parity on DG**x**LD**y** aborted				
Description	Reg. parity on **dg**x**ld**y was aborted.				
Advice	Check if the logic disk is busy or non-optimal.				

Event ID	0x203f				
Type	TASK	**Severity**	INFO	**Parameters**	DG ID, LD_ID
Message	Reg. parity on DG**x**LD**y** stopped				
Description	Reg. parity on **dg**x**ld**y was stopped manually.				
Advice	None				

Event ID	0x203d				
Type	TASK	**Severity**	NOTICE	**Parameters**	DG ID, LD_ID
Message	Reg. parity on DG**x**LD**y** completed				
Description	Reg. parity on **dg**x**ld**y was completed.				
Advice	None				

Event ID	0x206d				
Type	TASK	**Severity**	NOTICE	**Parameters**	Reg. Prog-ress, DG ID, LD_ID, Notify threshold
Message	Reg. progress(**w**%) on DG**x**LD**y** reach to the notify percent(**z**%)				
Description	The progress of Reg. parity on **dg**x**ld**y has reached the pre-define threshold.				
Advice	None				

D.3 Disk

- **Disk status**

Event ID	0x0811				
Type	DISK	**Severity**	INFO	**Parameters**	Disk ID
Message	HDD**x** powered on/off				
Description	**hdd**x was powered on or off.				
Advice	None				

Event ID	0x0817				
Type	DISK	**Severity**	ERROR	**Parameters**	Disk ID
Message	HDD**x** failed				
Description	**hdd**x failed to respond to the controller.				
Advice	Check if the disk is corrupt or the disk interface connection is unstable.				

Event ID	0x0810				
Type	DISK	**Severity**	WARNING	**Parameters**	Disk ID
Message	HDD**x** issued SMART warning				
Description	Controller detects that **hdd**x is signaling SMART warning.				
Advice	The disk is failing or will fail in the near term, replace the hard disk.				

- **Disk IO exception handling**

Event ID	0x0818				
Type	DISK	**Severity**	NOTICE	**Parameters**	Controller ID, Disk ID
Message	Controller **x** detected CRC error on HDD**y**				
Description	The controller **x** detected a CRC error when transferring data with **hdd**y. This could be a transient error due to unstable channel, electronic interference, heavy traffic, or malfunctioning hard disks. The controller will invalidate the data and retry the command.				
Advice	If this event occurs often, check the disk connectivity, check power supply to disks, or replace with a new disk.				

Event ID	0x0819				
Type	DISK	**Severity**	NOTICE	**Parameters**	Controller ID, Disk ID
Message	Controller **x** detected aborted task on HDD**y**				
Description	The controller **x** aborted the command that **hdd**y failed to respond to controller in time. This could be a transient error due to unstable channel, heavy traffic, or malfunctioning hard disks. The controller will retry the command to complete the IO; however, this could result in performance drop of the disk.				
Advice	If this event occurs often, check the disk connectivity, check power supply to disks, or replace with a new disk.				

Event ID	0x081a				
Type	DISK	**Severity**	WARNING	**Parameters**	Controller ID, Disk ID
Message	Controller **x** resets on HDD**y**				
Description	The controller **x** resets **hdd**y that failed to respond to controller in time and forced the disk back to its initial state. This could be a transient error due to unstable channel, heavy traffic, or malfunctioning hard disks. The controller will resume normal access to the disk after resetting the disk; however, this could result in performance drop of the disk. If the disk cannot resume normal opera-				
Advice	If this event occurs often, check the disk connectivity, check power supply to disks, or replace with a new disk.				

Event ID	0x081e				
Type	DISK	**Severity**	NOTICE	**Parameters**	DISK ID, opcode, sense key, ASC, ASCQ
Message	Check condition on HDDv: SCSI opcode=w, Sense Key=x, ASC=y, ASCQ=z				
Description	This presents the SCSI status number when error happens such as CRC error and it will have some field (Sense Key, ASC, ASCQ).				
Advice	If this event occurs often, check the disk connectivity, check power supply to disks, or replace with a new disk.				

Event ID	0x0813				
Type	DISK	**Severity**	NOTICE	**Parameters**	Controller ID, DISK ID, Error Code
Message	Controller **x** detected gross error on HDD**y** with code **z**				
Description	The controller **x** makes gross error on **hdd**y, with parameter code **z**. This could be transient error due to unstable channel, electronic interference, heavy traffic, casually misbehaved hard disks, or old FW. The controller will invalidate the data and retry the command.				
Advice	If this event occurs often, check the disk connectivity, check power supply to disks, replace with a new disk, or contact local sales or support office.				

- Disk port and chip

Event ID	0x081b				
Type	DISK	**Severity**	ERROR	**Parameters**	Disk port ID, Controller ID
Message	Reset disk port **x** in controller **y**				
Description	The controller **y** resets disk port **x** that failed to execute commands properly. This could be a transient error due to unstable channel, heavy traffic, or malfunctioning hard disks. The controller will resume normal operations after reset; however, this could result in performance drop of the disks attached to the disk port.				
Advice	If this event occurs often, check the disk connectivity, check power supply to disks, or replace with a new disk.				

Event ID	0x081c				
Type	DISK	**Severity**	WARNING	**Parameters**	Chip ID, Controller ID
Message	Reset disk i/f chip **x** in controller **y**				
Description	The controller **y** resets chip **x** that failed to execute commands properly. This could be a transient error due to unstable channel, heavy traffic, or malfunctioning hard disks. The controller will resume normal operations of the chip after reset; however, this could result in performance drop of the disks attached to the disk ports of this chip.				
Advice	If this event occurs often, check the disk connectivity, check power supply to disks, or replace with a new disk.				

Event ID	0x081d				
Type	DISK	**Severity**	FATAL	**Parameters**	Chip ID, Controller ID
Message	Disk i/f chip **x** in controller **y** failed				
Description	The controller **y** cannot execute commands properly on chip **x** after all appropriate recovery procedures were conducted. This could be the result of unstable power supply to the system. All disks controlled by the chip will fail.				
Advice	Check power supply, replace with a new controller, or contact local sales or support office.				

Event ID	0x081f				
Type	DISK	**Severity**	ERROR	**Parameters**	Disk Channel ID, Controller ID, Register value
Message	Disk channel **x** in controller **y** PCI Error cause register: **z**				
Description	The controller **y** has detected error in the disk channel.				
Advice	Check if the power supply is stable. Contact local sales or support office.				

- SMART disk self tests

Event ID	0x0807				
Type	DISK	**Severity**	INFO	**Parameters**	Disk ID
Message	SHT DST on HDD**x** started				
Description	**hdd**x started SMART short device self test routine.				
Advice	None				

Event ID	0x0806				
Type	DISK	**Severity**	INFO	**Parameters**	Disk ID
Message	EXT DST on HDD**x** started				
Description	**hdd**x started SMART extended device self test routine.				
Advice	None				

Event ID	0x0808				
Type	DISK	**Severity**	INFO	**Parameters**	Disk ID
Message	DST on HDD**x** stopped				
Description	DST on **hdd**x was stopped by the controller or from the user interface.				
Advice	None				

Event ID	0x0809				
Type	DISK	**Severity**	NOTICE	**Parameters**	Disk ID
Message	DST on HDD**x** completed without error				
Description	DST on **hdd**x completed without error.				
Advice	None				

Event ID	0x080a				
Type	DISK	**Severity**	WARNING	**Parameters**	Disk ID
Message	DST on HDD**x** unable to complete due to fatal error				
Description	DST on **hdd**x unable to complete due to fatal error.				
Advice	The disk failed or will fail soon, replace the hard disk.				

Event ID	0x080b				
Type	DISK	**Severity**	WARNING	**Parameters**	Disk ID
Message	DST on HDD**x** completed with read error				
Description	DST on **hdd**x completed with read error.				
Advice	The disk failed or will fail soon, replace the hard disk.				

Event ID	0x080c				
Type	DISK	**Severity**	WARNING	**Parameters**	Disk ID
Message	DST on HDD**x** completed with servo error				
Description	DST on **hdd**x completed with servo error.				
Advice	The disk failed or will fail soon, replace the hard disk.				

Event ID	0x080d				
Type	DISK	**Severity**	WARNING	**Parameters**	Disk ID
Message	DST on HDD**x** completed with electrical error				
Description	DST on **hdd**x completed with electrical error.				
Advice	The disk failed or will fail soon, replace the hard disk.				

Event ID	0x080e				
Type	DISK	**Severity**	WARNING	**Parameters**	Disk ID
Message	DST on HDD**x** completed with unknown test element error				
Description	DST on **hdd**x completed with error but the failed elements are unknown.				
Advice	The disk failed or will fail soon, replace the hard disk.				

- Bad block handling

Event ID	0x1401				
Type	DISK	**Severity**	WARNING	**Parameters**	Start Sector NO, End Sector NO, Disk ID
Message	Bad blocks between sector **x** and sector **y** on HDD**z** detected				
Description	A bad block starting from sector **x** on hdd**y** was detected by the controller.				
Advice	If the number of bad blocks detected is growing exceptionally fast or beyond a reasonable number, consider to conduct diagnostics and replace with new disks. If there is no subsequent event notifying the recovery or reallocation of the bad block detected, data on the bad block is lost.				

Event ID	0x1404				
Type	DISK	**Severity**	WARNING	**Parameters**	Start Sector NO, End Sector NO, Disk ID
Message	Bad blocks between sector **x** and sector **y** on HDD**z** recovered				
Description	A bad block starting from sector **x** on hdd**y** was recovered by the controller.				
Advice	If the number of bad blocks detected grows exceptionally fast or beyond a reasonable number, consider to conduct diagnostics and replace with new disks.				

Event ID	0x1400				
Type	DISK	**Severity**	WARNING	**Parameters**	Sector NO, Sector NO, Disk ID
Message	A BBR entry added for mapping sector **x** to sector **y** on HDD**z**				
Description	An entry of bad block reallocation table at was allocated for mapping sector **x** to sector **y** on hdd**z**.				
Advice	If the number of BBR table entries or spare blocks being reallocated grows exceptionally fast or beyond a reasonable number, consider to conduct diagnostics and replace with new disks.				

Event ID	0x1408				
Type	DISK	**Severity**	WARNING	**Parameters**	Sector NO, Disk ID
Message	Invalidate sector **x** on HDD**y**				
Description	The controller marks an area starting from sector **x** on hdd**y** as non-trustable by recording the sector in the bad block reallocation table. When the controller accesses the invalidated areas, it returns media error to hosts. This happens when the controller cannot rebuild data from remaining disks (This results in data loss), but the area on disk is still accessible. The mark could be removed when hosts writes to this area or corresponding logical disk is re-created.				
Advice	If the number of BBR table entries being allocated grows exceptionally fast or beyond a reasonable number, consider to conduct diagnostics and replace with new disks.				

Event ID	0x140e				
Type	DISK	**Severity**	WARNING	**Parameters**	Sector NO, Disk ID
Message	Read from an invalidated block at sector **x** on HDD**y**				
Description	The hosts read data from sector **x** on hdd**y** which was previously marked an invalidated area. The hosts got media error from the controller. This happens when the controller cannot rebuild data from remaining disks (This results in data loss), but the area on disk is still accessible.				
Advice	If the number of BBR table entries being allocated grows exceptionally fast or beyond a reasonable number, consider to conduct diagnostics and replace with new disks.				

Event ID	0x1409				
Type	DISK	**Severity**	NOTICE	**Parameters**	Threshold value, Disk ID
Message	BBR exceeds notice threshold **x**% on HDD**y**				
Description	The number of bad block reallocation table entries on hdd**y** has exceeded the pre-defined threshold level. The severity of this event depends on the threshold being exceed. Over threshold 1/ 2/3 leads to notice events.				
Advice	If the number of BBR table entries or spare blocks being reallo-cated grows exceptionally fast or beyond a reasonable number, consider to conduct diagnostics and replace with new disks.				

Event ID	0x140a				
Type	DISK	**Severity**	WARNING	**Parameters**	Threshold value, Disk ID
Message	BBR exceeds warning threshold **x**% on HDD**y**				
Description	The number of bad block reallocation table entries on hdd**y** has exceeded the pre-defined threshold level. The severity of this event depends on the threshold being exceed. Over threshold 4 leads to warning events.				
Advice	If the number of BBR table entries or spare blocks being reallo-cated grows exceptionally fast or beyond a reasonable number, consider to conduct diagnostics and replace with new disks.				

Event ID	0x140d				
Type	DISK	**Severity**	NOTICE	**Parameters**	Disk ID
Message	BBR exceeds clone threshold on HDD**x**				
Description	The number of bad block reallocation table entries on hdd**x** has exceeded the pre-defined threshold level to trigger disk cloning.				
Advice	If the number of BBR table entries or spare blocks being reallo-cated grows exceptionally fast or beyond a reasonable number, consider to conduct diagnostics and replace with new disks.				

Event ID	0x1402				
Type	DISK	**Severity**	WARNING	**Parameters**	Disk ID
Message	Out of BBR table entries on HDD**x**				
Description	All entries of the bad block reallocation table were occupied, and neither reallocation nor block invalidation could be done if new bad sectors are detected.				
Advice	Replace with new disks to prevent data loss.				

Event ID	0x1403				
Type	DISK	**Severity**	WARNING	**Parameters**	Disk ID
Message	Out of BBR spare blocks on HDD**x**				
Description	On-disk reserved space for bad block reallocation was occupied, reallocation cannot proceed if new bad sectors are detected.				
Advice	Replace with new disks to prevent from data loss.				

- On-disk metadata

Event ID	0x0814				
Type	DISK	**Severity**	WARNING	**Parameters**	Disk ID
Message	Write primary metadata on HDD**x** failed				
Description	The controller failed to access the primary RAID metadata stored on hdd**x** and the metadata was non-trustable. However, the secondary RAID metadata still works.				
Advice	Start to monitor more carefully the status of the secondary RAID metadata on this disk.				

Event ID	0x0815				
Type	DISK	**Severity**	WARNING	**Parameters**	Disk ID
Message	Write secondary metadata on HDD**x** failed				
Description	The controller failed to access the secondary RAID metadata stored on hdd**x** and the metadata was invalid. However, the primary RAID metadata still works.				
Advice	Start to monitor more carefully the status of the primary RAID metadata on this disk.				

Event ID	0x0816				
Type	DISK	**Severity**	WARNING	**Parameters**	Disk ID
Message	Write both metadata on HDD**x** failed				
Description	The controller failed to access both primary and secondary RAID metadata on hdd**x**, and the RAID metadata was invalid. In this case, **hdd**x will be set to faulty, and disk rebuilding will be started, if needed.				
Advice	None				

Event ID	0x0821				
Type	DISK	**Severity**	WARNING	**Parameters**	Disk ID
Message	Read primary metadata on HDD**x** failed				
Description	The controller failed to access the primary RAID metadata stored on hdd**x** and the metadata was non-trustable. However, the secondary RAID metadata still works.				
Advice	Start to monitor more carefully the status of the secondary RAID metadata on this disk.				

Event ID	0x0822				
Type	DISK	**Severity**	WARNING	**Parameters**	Disk ID
Message	Read both metadata on HDD**x** failed				
Description	The controller failed to access both primary and secondary RAID metadata on hdd**x**, and the RAID metadata was non-trustable. In this case, **hdd**x will be set to faulty, and disk rebuilding will be started, if needed.				
Advice	Start to monitor more carefully the status of the primary RAID metadata on this disk.				

Event ID	0x0823				
Type	DISK	**Severity**	WARNING	**Parameters**	Disk ID
Message	Primary metadata checksum error on HDD**x** failed				
Description	The primary RAID metadata stored on hdd**x** was non-trustable. However, the secondary RAID metadata still works.				
Advice	None				

Event ID	0x0824				
Type	DISK	**Severity**	WARNING	**Parameters**	Disk ID
Message	Secondary metadata checksum error on HDD**x** failed				
Description	The secondary RAID metadata stored on hdd**x** was non-trust-able. However, the primary RAID metadata still works.				
Advice	None				

Event ID	0x1405				
Type	DISK	**Severity**	WARNING	**Parameters**	Disk ID
Message	Primary BBR table on HDD**x** is corrupt				
Description	The controller failed to access the primary BBR table on hdd**x** and the table was invalid. However, the secondary BBR table still works.				
Advice	Start to monitor the status of the secondary BBR table on this disk.				

Event ID	0x1406				
Type	DISK	**Severity**	WARNING	**Parameters**	Disk ID
Message	Secondary BBR table on HDD**x** is corrupt				
Description	The controller failed to access the secondary BBR table on hdd**x** and the table was non-trustable. However, the primary BBR table still works.				
Advice	Start to monitor more carefully the status of the primary BBR table on this disk.				

Event ID	0x1407				
Type	DISK	**Severity**	WARNING	**Parameters**	Disk ID
Message	Both BBR tables on HDD**x** are corrupt				
Description	The controller failed to access both primary and secondary BBR tables on hdd**x**, and the tables were non-trustable. In this case, the BBR functions cannot work any more.				
Advice	Replace with new disks to prevent from data loss.				

D.4 Host ports

FC

- Hosts

Event ID	0x3000				
Type	HOST	Severity	INFO	Parameters	Host WWPN, Host Port ID
Message	Host **x** detected on host port **y**				
Description	The controller detected host **x** on host port **y**. The host can start access the controller over the host port.				
Advice	None				

Event ID	0x3001				
Type	HOST	Severity	NOTICE	Parameters	Host WWPN, Host Port ID
Message	Host **x** removed on host port **y**				
Description	Host **x** quitted from host port **y**.				
Advice	If host quitted unexpectedly, or it happens continuously during host access, check the host connectivity, or contact local sales or support office.				

- Link

Event ID	0x3002				
Type	HOST	Severity	INFO	Parameters	Host Port ID
Message	Host port **x** link up				
Description	The link on the host port **x** had been built by the controller successfully, and data transferring can be started.				
Advice	None				

Event ID	0x3003				
Type	HOST	**Severity**	NOTICE	**Parameters**	Host Port ID
Message	Host port **x** link down				
Description	The link on the host port **x** had been turned down by the controller, and data transferring was posed. This happens when the host port was disconnected from host HBA or switch because of removing/powering down/resetting the host or switch, or removing the cables.				
Advice	If the link unexpectedly disconnects, or it happens continuously during host access, check the host connectivity, or contact local sales or support office.				

- IO exceptions handling

Event ID	0x3004				
Type	HOST	**Severity**	NOTICE	**Parameters**	Host Port ID
Message	LIP issued on host port **x**				
Description	The controller issued LIP (Loop Initialization Packet) on host port **x**. This is to ask host to rescan the connection and get updated of LUN information, such as capacity change or LUN mapping change.				
Advice	None				

Event ID	0x3005				
Type	HOST	**Severity**	WARNING	**Parameters**	Host Port ID
Message	LIP detected on host port **x**				
Description	The controller detected LIP (Loop Initialization Packet) on host port **x**. This could be to recover from a transient error due to unstable channel, command time-out, or unexpected host behaviors. The controller will drop the command specified by the host, and the host will retry the command.				
Advice	None				

Event ID	0x3006				
Type	HOST	Severity	WARNING	Parameters	Host Port ID, Host WWPN, LUN ID
Message	Task abort on host port **x** from host **y** to LUN **z**				
Description	The controller received task abort on host port **x** from host **y** to LUN **z**. This could be to recover from a transient error due to unstable channel, command time-out, or unexpected host behaviors. The controller will drop the command specified by the host, and the host will retry the command; however, this could result in LUN performance drop.				
Advice	If this event occurs often, check the host connectivity, check LUN's IO statistics to see if the maximum response time is reasonable for the hosts connected, or contact local sales or support office.				

- Port and chip

Event ID	0x3007				
Type	HOST	Severity	INFO	Parameters	Host Port ID
Message	Host port **x** started				
Description	The controller has started the host port **x** successfully, and link-up can be started.				
Advice	None				

Event ID	0x3008				
Type	HOST	Severity	WARNING	Parameters	Host Port ID
Message	Port reset detected on host port **x**				
Description	The controller detected port reset on host port **x**. This could be to recover from transient error due to a unstable channel, command time-out, or unexpected host behaviors. The controller will drop the command specified by the host, and the host will retry the command; however, this could result in performance drop of the LUNs exported to the host ports of this chip.				
Advice	If this event occurs often, check the host connectivity, check LUN's IO statistics to see if the maximum response time is reasonable for the hosts connected, or contact local sales or support office.				

Event ID	0x3009				
Type	HOST	**Severity**	WARNING	**Parameters**	Chip ID, Controller ID
Message	Reset host i/f chip **x** in controller **y**				
Description	The controller resets chip **x** that failed to execute commands properly. This could be to recover from a transient error due to unstable channel or heavy traffic. The controller will resume normal operations of the chip after reset; however, this could result in performance drop of the LUNs exported to the host ports of this chip.				
Advice	If this event occurs often, check the host connectivity, or contact local sales or support office.				

Event ID	0x300a				
Type	HOST	**Severity**	FATAL	**Parameters**	Chip ID, Controller ID
Message	Host i/f chip **x** in controller **y** failed				
Description	The controller cannot execute commands properly on chip **x** after all appropriate recovery procedures were conducted. This could be resulted from unstable power supply to the system. All LUNs controlled by the chip will be unavailable to hosts.				
Advice	Check power supply, replace with a new controller, or contact local sales or support office.				

Event ID	0x300b				
Type	HOST	**Severity**	ERROR	**Parameters**	Host Channel ID, Controller ID, Error Code
Message	Host channel **x** in controller **y** PCI Error: **z**				
Description	The controller has detected error in the host channel.				
Advice	Check if the power supply is stable. Contact local sales or support office.				

SAS

- Hosts

Event ID	0x300c				
Type	HOST	**Severity**	INFO	**Parameters**	Host WWPN, Host Port ID
Message	Host **x** detected on host port **y**				
Description	The controller detected host **x** on host port **y**. The host can start access the controller over the host port.				
Advice	None				

- Link

Event ID	0x300d				
Type	HOST	**Severity**	INFO	**Parameters**	Host Port ID, phy ID
Message	Host port **x** phy **y** link up				
Description	The link on the host port **x** phy **y** had been built by the controller successfully, and data transferring can be started.				
Advice	None				

Event ID	0x300e				
Type	HOST	**Severity**	NOTICE	**Parameters**	Host Port ID, phy ID
Message	Host port **x** phy **y** link down				
Description	The link on the host port **x** phy **y** had been turned down by the controller, and data transferring was posed. This happens when the host port was disconnected from host HBA or switch because of removing/powering down/resetting the host or switch, or removing the cables.				
Advice	If the link unexpectedly disconnects, or it happens continuously during host access, check the host connectivity, or contact local sales or support office.				

- IO exceptions handling

Event ID	0x300f				
Type	HOST	**Severity**	WARNING	**Parameters**	Host Port ID, Host WWPN, LUN ID
Message	Task abort on host port **x** from host **y** to LUN **z**				
Description	The controller received task abort on host port **x** from host **y** to LUN **z**. This could be to recover from a transient error due to unstable channel, command time-out, or unexpected host behaviors. The controller will drop the command specified by the host, and the host will retry the command; however, this could result in LUN performance drop.				
Advice	If this event occurs often, check the host connectivity, check LUN's IO statistics to see if the maximum response time is reasonable for the hosts connected, or contact local sales or support office.				

- Port and chip

Event ID	0x3010				
Type	HOST	**Severity**	INFO	**Parameters**	Host Port ID
Message	Host port **x** started				
Description	The controller has started the host port **x** successfully, and link-up can be started.				
Advice	None				

Event ID	0x3011				
Type	HOST	**Severity**	WARNING	**Parameters**	Controller ID, Chip ID
Message	Reset host i/f chip **x** in controller **y**				
Description	The controller **y** resets chip **x** that failed to execute commands properly. This could be to recover from transient error due to a unstable channel or heavy traffic. The controller will resume normal operations of the chip after reset; however, this could result in performance drop of the LUNs exported to the host ports of this chip.				
Advice	If this event occurs often, check the host connectivity, or contact local sales or support office.				

Event ID	0x3012				
Type	HOST	**Severity**	ERROR	**Parameters**	Host Channel ID, Controller ID, Error Code
Message	Host channel **x** in controller **y** PCI Error: **z**				
Description	The controller **y** has detected error in the host channel.				
Advice	Check if the power supply is stable. Contact local sales or support office.				

Event ID	0x3013				
Type	HOST	**Severity**	WARNING	**Parameters**	Host Port ID
Message	IOC Bus Reset on port **x**				
Description	A bus reset has occurred on port **x** that was initiated by the IOC.				
Advice	None				

Event ID	0x3014				
Type	HOST	**Severity**	WARNING	**Parameters**	Host Port ID
Message	Ext Bus Reset on port **x**				
Description	A bus reset has occurred on port **x** that was initiated by an external entity.				
Advice	None				

SCSI

- IO exceptions handling

Event ID	0x3015				
Type	HOST	**Severity**	WARNING	**Parameters**	Host Port ID, Host SCSI ID, LUN ID
Message	Task abort on host port **x** from host **y** to LUN **z**				
Description	The controller received task abort on host port **x** from host **y** to LUN **z**. This could be to recover from a transient error due to unstable channel, command time-out, or unexpected host behaviors. The controller will drop the command specified by the host, and the host will retry the command; however, this could result in LUN performance drop.				
Advice	If this event occurs often, check the host connectivity, check LUN's IO statistics to see if the maximum response time is reasonable for the hosts connected, or contact local sales or support office.				

Event ID	0x3016				
Type	HOST	**Severity**	WARNING	**Parameters**	Host Port ID
Message	Host port **x** detected parity error during Command phase				
Description	Parity error was detected during command phase.				
Advice	None				

Event ID	0x3017				
Type	HOST	**Severity**	WARNING	**Parameters**	Host Port ID
Message	Host port **x** detected parity error during Message Out phase				
Description	Parity error was detected during message out phase.				
Advice	None				

Event ID	0x3018				
Type	HOST	**Severity**	WARNING	**Parameters**	Host Port ID
Message	Host port **x** detected CRC error while receiving CMD_IU				
Description	CRC error was detected while receiving CMD_IU.				
Advice	None				

Event ID	0x3019				
Type	HOST	Severity	WARNING	Parameters	Host Port ID
Message	Host port **x** detected parity error during Command phase				
Description	Parity error was detected during command phase.				
Advice	None				

Event ID	0x301a				
Type	HOST	Severity	WARNING	Parameters	Host Port ID
Message	Host port **x** detected parity error during Data Out phase				
Description	Parity error was detected during data out phase.				
Advice	None				

Event ID	0x301b				
Type	HOST	Severity	WARNING	Parameters	Host Port ID
Message	Host port **x** detected CRC error during Data Out phase				
Description	CRC error was detected during data out phase.				
Advice	None				

Event ID	0x301c				
Type	HOST	Severity	WARNING	Parameters	Host Port ID
Message	Host port **x** transfer count mismatch				
Description	The amount of data that the target actually transferred does not match the DataLength. The amount of data was specified in the TargetAssist request message.				
Advice	None				

Event ID	0x301d				
Type	HOST	Severity	WARNING	Parameters	Host Port ID
Message	Host port **x** data offset error				
Description	Data was received with a data offset that was not expected.				
Advice	None				

Event ID	0x301e				
Type	HOST	Severity	WARNING	Parameters	Host Port ID
Message	Host port **x** too much write data				
Description	More than the expected amount of write data was received from the initiator.				
Advice	None				

Event ID	0x301f				
Type	HOST	Severity	WARNING	Parameters	Host Port ID
Message	Host port **x** IU too short				
Description	A received information unit was shorter than the value allowed by the protocol specification.				
Advice	None				

Event ID	0x3020				
Type	HOST	Severity	WARNING	Parameters	Host Port ID
Message	Host port **x** EEDP Guard Error				
Description	The data in an end-to-end data protection I/O failed the CRC guard check.				
Advice	None				

Event ID	0x3021				
Type	HOST	Severity	WARNING	Parameters	Host Port ID
Message	Host port **x** EEDP Reference Tag Error				
Description	The logical block reference tag in the data protection information block of an end-to-end data protection I/O did not match the expected value.				
Advice	None				

Event ID	0x3022				
Type	HOST	Severity	WARNING	Parameters	Host Port ID
Message	Host port **x** EEDP Application Tag Error				
Description	The logical block application tag in the data protection information block of an end-to-end data protection I/O did not match the expected value.				
Advice	None				

- Port and chip

Event ID	0x3023				
Type	HOST	**Severity**	WARNING	**Parameters**	Host Port ID
Message	IOC Bus Reset on port **x**				
Description	A bus reset has occurred on port **x** that was initiated by the IOC.				
Advice	None				

Event ID	0x3024				
Type	HOST	**Severity**	WARNING	**Parameters**	Host Port ID
Message	Ext Bus Reset on port **x**				
Description	A bus reset has occurred on port **x** that was initiated by an external entity.				
Advice	None				

D.5 Controller hardware

- Memory

Event ID	0x241e				
Type	CONTROLLER	**Severity**	WARNING	**Parameters**	Controller ID, Single-bit error address
Message	Memory ECC single-bit error in controller **x**: **y**				
Description	The controller **x** has detected and corrected single-bit error in the memory module.				
Advice	Check if the memory module is installed properly, and make sure the memory module is in the compatibility list. Replace the memory module, and if the error continuously happens, contact local sales or support office.				

- Flash chip

Event ID	0x2421				
Type	CONTROLLER	**Severity**	ERROR	**Parameters**	Controller ID
Message	Primary system flash in controller **x** is corrupt				
Description	The primary system flash chip on controller **x** is corrupt and cannot be used. But the secondary flash still works.				
Advice	Check if there are any hardware hazards that lead to abnormal flash corruption. Watch the secondary flash chip.				

Event ID	0x2422				
Type	CONTROLLER	**Severity**	ERROR	**Parameters**	Controller ID
Message	Secondary system flash in controller **x** is corrupt				
Description	The secondary system flash chip on controller **x** is corrupt and cannot be used. But the primary flash still works.				
Advice	Check if there are any hardware hazards that lead to abnormal flash corruption. Watch the secondary flash chip.				

Event ID	0x242b				
Type	CONTROLLER	**Severity**	ERROR	**Parameters**	Controller ID
Message	Bootrom in controller **x** is corrupt				
Description	Bootrom on controller **x** is corrupt and cannot be used. Because the bootcode is stored on the bootrom, the controller cannot work.				
Advice	Check if the power supply is stable. Replace with a new controller. Contact local sales or support office.				

Event ID	0x2423				
Type	CONTROLLER	**Severity**	INFO	**Parameters**	Bad block number, Controller ID
Message	Bad block **x** on primary system flash added in controller **y**				
Description	Bad blocks happened and remapped successfully on the primary system flash in controller **y**.				
Advice	Check if there are any hardware hazards that lead to abnormal flash corruption. Watch the secondary flash chip.				

Event ID	0x2424				
Type	CONTROLLER	**Severity**	INFO	**Parameters**	Bad block number, Controller ID
Message	Bad block **x** on secondary system flash added in controller **y**				
Description	Bad blocks happened and remapped successfully on the secondary system flash in controller **y**.				
Advice	Check if there are any hardware hazards that lead to bad blocks. Watch the secondary flash chip.				

Event ID	0x2425				
Type	CONTROLLER	**Severity**	WARNING	**Parameters**	Controller ID
Message	Bad block on primary system flash over 70% in controller **y**				
Description	The amount of bad blocks is over 70% of the table that is used to remap bad blocks.				
Advice	Check if there are any hardware hazards that lead to bad blocks. This flash chip is close to fail.				

Event ID	0x2426				
Type	CONTROLLER	**Severity**	WARNING	**Parameters**	Controller ID
Message	Bad block on secondary system flash over 70% in controller **y**				
Description	The amount of bad blocks is over 70% of the table that is used to remap bad blocks.				
Advice	Check if there are any hardware hazards that lead to bad blocks. This flash chip is close to fail.				

- Controller (In Dual-Controller Configuration)

Event ID	0x242e				
Type	CONTROLLER	**Severity**	ERROR	**Parameters**	Controller ID
Message	Controller **x** failed				
Description	One of the controllers failed, was removed, or powered off, while the other controller remains working. This happens only in dual-controller configuration.				
Advice	Check if the power supply is stable. Replace with a new controller.				

Event ID	0x242f				
Type	CONTROLLER	**Severity**	ERROR	**Parameters**	Controller ID
Message	Controller **x** returned				
Description	The failed controller has been replaced and back to work.				

D.6 Enclosure

- **Temperature**

Event ID	0x2800				
Type	ENCLOSURE	**Severity**	NOTICE	**Parameters**	Sensor ID, Enclosure ID, Temperature
Message	Temperature at sensor **x** in enclosure **y** back to normal (**z** C) Temperature at sensor **x** in controller back to normal (**z** C)				
Description	The temperature at sensor **x** in enclosure **y** or controller returned to normal working temperature range, right now is **z** °C.				
Advice	If the temperature is very unstable, contact local sales or support office.				

Event ID	0x2801				
Type	ENCLOSURE	**Severity**	WARNING	**Parameters**	Sensor ID, Enclosure ID, Temperature
Message	Abnormal temperature detected by sensor **x** in enclosure **y** (**z** C) Abnormal temperature detected by sensor **x** in controller (**z** C)				
Description	The temperature at sensor **x** in enclosure **y** or controller has been out of normal working temperature range, right now is **z** °C.				
Advice	Check the fans in the system and the air conditioning of the environment.				

Event ID	0x2802				
Type	ENCLOSURE	**Severity**	ERROR	**Parameters**	Sensor ID, Enclosure ID
Message	The temperature sensor **x** in enclosure **y** failed The temperature sensor **x** in controller failed				
Description	The controller cannot detect the temperature sensor **x** in enclosure **y** or controller.				
Advice	Contact local sales or support office.				

- Fan

Event ID	0x2804				
Type	ENCLOSURE	**Severity**	NOTICE	**Parameters**	Fan ID, Enclosure ID
Message	Rotation speed of fan **x** in enclosure **y** back to normal				
Description	The rotation speed of fan **x** in enclosure **y** returned to normal range.				
Advice	If the rotation speed is very unstable, replace the fan, or contact local sales or support office.				

Event ID	0x2805				
Type	ENCLOSURE	**Severity**	WARNING	**Parameters**	Fan ID, Enclosure ID
Message	Abnormal rotation speed of fan **x** in enclosure **y** detected.				
Description	The rotation speed of fan **x** in enclosure **y** has been out of normal range.				
Advice	Replace the fan, or contact local sales or support office.				

- Voltage

Event ID	0x2807				
Type	ENCLOSURE	**Severity**	NOTICE	**Parameters**	Voltage
Message	+3.3V voltage source in backplane back to normal (**z** V) +3.3V voltage source in controller back to normal (**z** V)				
Description	+3.3V voltage source in backplane or controller returned to normal range, right now is **z**V.				
Advice	If the voltage is very unstable, contact local sales or support office.				

Event ID	0x2808				
Type	ENCLOSURE	**Severity**	NOTICE	**Parameters**	Voltage
Message	+5V voltage source in backplane back to normal (**z** V) +5V voltage source in controller back to normal (**z** V)				
Description	+5V voltage source in backplane or controller returned to normal range, right now is **z**V.				
Advice	If the voltage is very unstable, contact local sales or support office.				

Event ID	0x2809				
Type	ENCLOSURE	**Severity**	NOTICE	**Parameters**	Voltage
Message	+12V voltage source in backplane back to normal (**z** V) +12V voltage source in controller back to normal (**z** V)				
Description	+12V voltage source in backplane or controller returned to normal range, right now is **z**V.				
Advice	If the voltage is very unstable, contact local sales or support office.				

Event ID	0x280a				
Type	ENCLOSURE	**Severity**	WARNING	**Parameters**	Voltage
Message	Abnormal +3.3V voltage source in backplane (**z** V) Abnormal +3.3V voltage source in controller (**z** V)				
Description	The current voltage of the +3.3V voltage source in backplane or controller was out of normal range, right now is **z**V.				
Advice	Check the power supply system, or contact local sales or support office.				

Event ID	0x280b				
Type	ENCLOSURE	**Severity**	WARNING	**Parameters**	Voltage
Message	Abnormal +5V voltage source in backplane (**z** V) Abnormal +5V voltage source in controller (**z** V)				
Description	The current voltage of the +5V voltage source in backplane or controller was out of normal range, right now is **z**V.				
Advice	Check the power supply system, or contact local sales or support office.				

Event ID	0x280c				
Type	ENCLOSURE	**Severity**	WARNING	**Parameters**	Voltage
Message	Abnormal +12V voltage source in backplane (**z** V) Abnormal +12V voltage source in controller (**z** V)				
Description	The current voltage of the +12V voltage source in backplane or controller was out of normal range, right now is **z**V.				
Advice	Check the power supply system, or contact local sales or support office.				

Event ID	0x2821				
Type	ENCLOSURE	**Severity**	NOTICE	**Parameters**	Voltage, Enclosure ID
Message	Voltage source **x** in enclosure **y** back to normal				
Description	Voltage source **x** in enclosure **y** returned to normal range.				
Advice	If the voltage is very unstable, contact local sales or support office.				

Event ID	0x2822				
Type	ENCLOSURE	**Severity**	WARNING	**Parameters**	Voltage ID, Enclosure ID, Voltage
Message	Abnormal voltage source **x** in enclosure **y** (**z** V)				
Description	Voltage source **x** in enclosure **y** was out of normal range.				
Advice	Check the power supply system, or contact local sales or support office.				

- Power supply

Event ID	0x280d				
Type	ENCLOSURE	**Severity**	INFO	**Parameters**	PSU ID, Enclosure ID
Message	Power supply **x** in enclosure **y** detected				
Description	Power supply unit (PSU) **x** was installed and present.				
Advice	None				

Event ID	0x280e				
Type	ENCLOSURE	**Severity**	ERROR	**Parameters**	PSU ID, Enclosure ID
Message	Power supply **x** in enclosure **y** failed				
Description	The controller cannot get status from power supply unit (PSU) **x** in enclosure **y**, which might have failed or removal.				
Advice	Replace the power supply, or contact local sales or support office.				

- BBM

Event ID	0x280f				
Type	ENCLOSURE	Severity	INFO	Parameters	
Message	BBM disabled				
Description	The battery backup function was disabled.				
Advice	None				

Event ID	0x2810				
Type	ENCLOSURE	Severity	INFO	Parameters	
Message	Dirty boot and flush data				
Description	The controller was not properly shutdown and it will flush cached data in memory protected by BBM.				
Advice	None				

Event ID	0x2811				
Type	ENCLOSURE	Severity	INFO	Parameters	
Message	Dirty-boot data flush completed				
Description	The data flush was completed, and the controller will restart and return to normal state.				
Advice	None				

Event ID	0x2812				
Type	ENCLOSURE	Severity	INFO	Parameters	Controller ID
Message	BBM in controller **x** is charging				
Description	BBM in controller **x** was not fully charged, and it started charging.				
Advice	Start host access or operations after the BBM at fully-charged state.				

Event ID	0x2813				
Type	ENCLOSURE	Severity	NOTICE	Parameters	Controller ID
Message	BBM in controller **x** charging completed				
Description	BBM in controller **x** charging was done and BBM was fully charged.				
Advice	None				

Event ID	0x2814				
Type	ENCLOSURE	**Severity**	WARNING	**Parameters**	Controller ID
Message	BBM in controller **x** absent				
Description	The controller **x** cannot detect BBM.				
Advice	Check if the BBM is properly installed or replace with a new BBM.				

Event ID	0x2815				
Type	ENCLOSURE	**Severity**	NOTICE	**Parameters**	Controller ID
Message	Temperature of BBM in controller **x** back to normal				
Description	The temperature of BBM in controller **x** returned to normal working temperature range.				
Advice	If the temperature is very unstable, contact local sales or support office.				

Event ID	0x2816				
Type	ENCLOSURE	**Severity**	WARNING	**Parameters**	Controller ID
Message	Abnormal temperature of BBM in controller **x**				
Description	The current temperature of BBM in controller **x** was out of normal range.				
Advice	Check the system fans and the air conditioning.				

- UPS

Event ID	0x2817				
Type	ENCLOSURE	**Severity**	INFO	**Parameters**	
Message	UPS connection detected				
Description	UPS detected by the controller.				
Advice	None				

Event ID	0x2818				
Type	ENCLOSURE	**Severity**	WARNING	**Parameters**	
Message	UPS connection loss				
Description	The controller cannot detect UPS.				
Advice	Make sure that the proper communication cable is securely connected to the UPS.				

Event ID	0x2819				
Type	ENCLOSURE	Severity	WARNING	Parameters	
Message	UPS AC power failure				
Description	The AC line voltage has failed.				
Advice	Make sure it is not unplugged from its power source if utility power exist.				

Event ID	0x281a				
Type	ENCLOSURE	Severity	INFO	Parameters	
Message	UPS AC power back on-line				
Description	The AC line voltage back to normal.				
Advice	None				

Event ID	0x281b				
Type	ENCLOSURE	Severity	WARNING	Parameters	
Message	UPS low battery				
Description	UPS battery charge below normal range.				
Advice	None				

Event ID	0x281c				
Type	ENCLOSURE	Severity	INFO	Parameters	
Message	UPS battery back to normal				
Description	UPS battery charge back to normal range.				
Advice	None				

Event ID	0x281d				
Type	ENCLOSURE	Severity	WARNING	Parameters	
Message	UPS battery will fail				
Description	The UPS has a battery that will fail.				
Advice	Replace the UPS battery as soon as possible.				

Event ID	0x281e				
Type	ENCLOSURE	Severity	INFO	Parameters	
Message	UPS battery replace back to non-failure status				
Description	The UPS is replaced and back to non-failure status.				
Advice	None				

Event ID	0x281f				
Type	ENCLOSURE	Severity	WARNING	Parameters	
Message	UPS overload				
Description	The UPS overload.				
Advice	(1) If overload occurs immediately after connecting new equipment to the UPS, the UPS cannot support the new load. You must connect one or more devices to a second UPS, or replace the current UPS with a model that can support a larger load. (2) If the overload was not caused by adding new load equipment, run a UPS self-test to see if the problem clears. If the test fails (an overload still exists), close all open applications at the UPS load equipment and reboot the UPS. If the problem persists, disconnect all equipment from the UPS and reboot the UPS. If the overload still exists, the UPS needs to be repaired or replaced. Contact the UPS vendor support for assistance. If the problem is cleared, reconnect and turn on the load equipment, one piece at a time, to determine which piece of equipment caused the overload.				

Event ID	0x2820				
Type	ENCLOSURE	Severity	INFO	Parameters	
Message	UPS overload solved				
Description	The UPS overload solved.				
Advice	None				

D.7 System

- **Configurations**

Event ID	0x2400				
Type	SYSTEM	**Severity**	INFO	**Parameters**	DISK ID
Message	RAID configurations on HDD**x** erased				
Description	The RAID configurations stored on **hdd**x were erased. RAID configurations for the disk, such as JBOD disk, disk group, logical disk, and volume, is lost.				
Advice	Re-install the disk to the controller so that the controller can re-initialize it.				

Event ID	0x2401				
Type	SYSTEM	**Severity**	INFO	**Parameters**	
Message	RAID configurations on all disks erased				
Description	RAID configurations stored on all disks were erased. All RAID configurations are lost.				
Advice	Restart the controller so that all disks can be re-initialized all together.				

Event ID	0x2415				
Type	SYSTEM	**Severity**	INFO	**Parameters**	
Message	NVRAM configurations restore to default				
Description	The controller configurations stored on NVRAM were erased and restored to factory default.				
Advice	None				

Event ID	0x2416				
Type	SYSTEM	**Severity**	INFO	**Parameters**	DISK ID
Message	NVRAM configurations restored from HDD**x**				
Description	The NVRAM configurations were restored from **hdd**x.				
Advice	None				

Event ID	0x2417				
Type	SYSTEM	Severity	INFO	Parameters	
Message	NVRAM configurations restored from file				
Description	The configurations were restored from a file uploaded to the controller.				
Advice	None				

Event ID	0x2409				
Type	SYSTEM	Severity	FATAL	Parameters	
Message	NVRAM configuration checksum error				
Description	The checksum stored on NVRAM do not match the contents on NVRAM. This could happen if the controller was not properly shut-down. Because NVRAM configurations might be corrupt and cannot be trusted, all event logs are automatically erased.				
Advice	Restore the configurations from hard disks or by uploading the backed-up configuration file. If this event happens continuously, contact local sales or support office.				

Event ID	0x2431				
Type	SYSTEM	Severity	FATAL	Parameters	
Message	NVRAM mapping table checksum error				
Description	The checksum stored on NVRAM do not match the contents on NVRAM. This could happen if the controller was not properly shut-down. System will restore the default mapping table automati-cally.				
Advice	Start to monitor more carefully the status of the NVRAM.				

- Security control

Event ID	0x240d				
Type	SYSTEM	Severity	INFO	Parameters	
Message	Admin login				
Description	Administrator login to the controller.				
Advice	None				

Event ID	0x2410				
Type	SYSTEM	Severity	INFO	Parameters	
Message	Admin login failed				
Description	Administrator failed to login to the controller.				
Advice	Check if there is any unauthorized trial access to the controller or there are multiple administrator logins.				

Event ID	0x2427				
Type	SYSTEM	Severity	INFO	Parameters	
Message	User login				
Description	User login to the controller.				
Advice	None				

Event ID	0x2428				
Type	SYSTEM	Severity	INFO	Parameters	
Message	User login failed				
Description	User failed to login to the controller.				
Advice	Check if there is any unauthorized trial access to the controller.				

Event ID	0x240e				
Type	SYSTEM	Severity	INFO	Parameters	
Message	Service login				
Description	Service login to the controller.				
Advice	None				

Event ID	0x2411				
Type	SYSTEM	Severity	INFO	Parameters	
Message	Service login failed				
Description	Service failed to login to the controller.				
Advice	Check if there is any unauthorized trial access to the controller.				

Event ID	0x240f				
Type	SYSTEM	Severity	INFO	Parameters	
Message	Accusys login				
Description	Accusys login to the controller.				
Advice	None				

Event ID	0x2412				
Type	SYSTEM	Severity	INFO	Parameters	
Message	Accusys login failed				
Description	Accusys failed to login to the controller.				
Advice	Check if there is any unauthorized trial access to the controller.				

- Events

Event ID	0x0400				
Type	SYSTEM	Severity	FATAL	Parameters	
Message	Event test with severity: fatal				
Description	Users have generated a simulated event to test the event handling/notification mechanisms. The severity level of this event is fatal.				
Advice	None				

Event ID	0x0401				
Type	SYSTEM	Severity	ERROR	Parameters	
Message	Event test with severity: error				
Description	Users have generated a simulated event to test the event handling/notification mechanisms. The severity level of this event is error.				
Advice	None				

Event ID	0x0402				
Type	SYSTEM	Severity	WARNING	Parameters	
Message	Event test with severity: warn				
Description	Users have generated a simulated event to test the event handling/notification mechanisms. The severity level of this event is warn.				
Advice	None				

Event ID	0x0403				
Type	SYSTEM	Severity	NOTICE	Parameters	
Message	Event test with severity: notice				
Description	Users have generated a simulated event to test the event handling/notification mechanisms. The severity level of this event is notice.				
Advice	None				

Event ID	0x0404				
Type	SYSTEM	Severity	INFO	Parameters	
Message	Event test with severity: info				
Description	Users have generated a simulated event to test the event handling/notification mechanisms. The severity level of this event is info.				
Advice	None				

Event ID	0x2406				
Type	SYSTEM	Severity	INFO	Parameters	
Message	All event logs erased				
Description	All event logs were erased. After that, this is the first event recorded.				
Advice	None				

Event ID	0x2413				
Type	SYSTEM	Severity	NOTICE	Parameters	
Message	Auto-write-through activated				
Description	The pre-defined triggering events for auto-write-through occurred, and the controller has set the buffer cache as write-through.				
Advice	Check the event logs, and remove the causes of events that trigger auto-write-through.				

Event ID	0x2414				
Type	SYSTEM	Severity	NOTICE	Parameters	
Message	Auto-write-through de-activated				
Description	The pre-defined triggering events for auto-write-through have gone, and the controller restored the original cache setting.				
Advice	None				

Event ID	0x2418				
Type	SYSTEM	Severity	NOTICE	Parameters	
Message	Auto-shutdown activated				
Description	The pre-defined triggering events for auto-shutdown occurred, and the controller was going to shutdown itself.				
Advice	Check the event logs, and remove the causes of events that trigger auto-shutdown. Restart the controller. Disable auto-shutdown first before starting investigating the causes.				

Event ID	0x2419				
Type	SYSTEM	Severity	FATAL	Parameters	
Message	NVRAM event log checksum error				
Description	The checksum stored on NVRAM for event log cannot match the contents on NVRAM. This could happen if the controller was not properly shutdown. Because the event log on NVRAM might be corrupt and cannot be trusted, all event logs will be erased automatically.				
Advice	If this event continuously happens, contact local sales or support office.				

- Firmware update

Event ID	0x2407				
Type	SYSTEM	Severity	INFO	Parameters	Controller ID
Message	System firmware in controller **x** updated				
Description	System firmware in controller **x** was updated successfully.				
Advice	Restart the controller so that the new firmware can be effective.				

Event ID	0x2408				
Type	SYSTEM	Severity	INFO	Parameters	Controller ID
Message	Controller **x** failed to update system firmware				
Description	The controller **x** cannot update the system firmware.				
Advice	Check the firmware file is not corrupt and has the correct version.				

Event ID	0x2429				
Type	SYSTEM	Severity	INFO	Parameters	Controller ID
Message	Boot code in controller **x** updated				
Description	Boot code in controller **x** was updated successfully.				
Advice	Restart the controller so that the new code can be effective.				

Event ID	0x242a				
Type	SYSTEM	Severity	INFO	Parameters	Controller ID
Message	Controller **x** failed to update boot code				
Description	The controller **x** cannot update the boot code.				
Advice	Check the firmware file is not corrupt and has the correct version.				

- Email (SMTP) server status

Event ID	0x240b				
Type	SYSTEM	Severity	WARNING	Parameters	
Message	Controller **x** failed to send mail				
Description	The controller failed to send mail. Both primary and secondary mail servers cannot be reached by the controller.				
Advice	Check if the network connection is up, and check if the network and SMTP settings are correct.				

Event ID	0x240a				
Type	SYSTEM	Severity	INFO	Parameters	
Message	Controller **x** sned mail back to normal				
Description	The controller can reach the mail server and start to send mail.				
Advice	None				

- System start-up and shutdown

Event ID	0x2402				
Type	SYSTEM	**Severity**	INFO	**Parameters**	
Message	System to be restarted or halted				
Description	The RAID system is going to get restarted or halted.				
Advice	None				

Event ID	0x2403				
Type	SYSTEM	**Severity**	INFO	**Parameters**	
Message	RAID system started				
Description	The RAID system was started.				
Advice	None				

- Miscellaneous

Event ID	0x240c				
Type	SYSTEM	**Severity**	ERROR	**Parameters**	Debug Code
Message	System error: **x**				
Description	Unknown system error, and its event ID is **x**.				
Advice	Contact local sales or support office.				

Event ID	0x2430				
Type	SYSTEM	**Severity**	FATAL	**Parameters**	Debug Code
Message	Fatal system fault: **x**				
Description	Unknown fatal system fault, and its event ID is **x**.				
Advice	Contact local sales or support office.				

D.8 Network

- Network

Event ID	0x3400				
Type	NETWORK	**Severity**	INFO	**Parameters**	Ethernet ID
Message	Link up on network interface **eth**x				
Description	The network link on network interface **eth**x had been built successfully.				
Advice	None				

Event ID	0x3401				
Type	NETWORK	**Severity**	NOTICE	**Parameters**	Ethernet ID
Message	Link down on network interface **eth**x				
Description	The network link on network interface of **eth**x had been turned down. This happens when the network configuration is incorrect, or cable were removed, or during abnormal network activity.				
Advice	If the network link unexpectedly disconnects, or it happens repeatedly, check the network configuration and hardware. If it is still unable to work, contact local sales or support office.				

Event ID	0x3402				
Type	NETWORK	**Severity**	WARNING	**Parameters**	Ethernet ID
Message	MAC address conflicted on network interface **eth**x				
Description	The MAC address of network adapter **eth**x conflicted with another one on the same network.				
Advice	Try to configure the network adaptor with a different MAC address.				

Event ID	0x3403				
Type	NETWORK	**Severity**	WARNING	**Parameters**	Ethernet ID
Message	IP address conflicted on network interface **eth**x				
Description	The IP address of network adapter **eth**x conflicted with another on the same network.				
Advice	Try to configure the network adaptor with different an IP address.				

D.9 Miscellaneous

- **Event subscribe**

Event ID	0x3800				
Type	MISC	**Severity**	NOTICE	**Parameters**	IP Address, Port Number
Message	Send message to **x** port **y** failed				
Description	Send a message a specify registrant is failed.				
Advice	None				

Event ID	0x3801				
Type	MISC	**Severity**	NOTICE	**Parameters**	IP Address, Port Number
Message	Registrant **x** port **y** is kicked				
Description	The registrant is kicked.				
Advice	None				

D.10 Snapshot

Event ID	0x3C00				
Type	SNAPSHOT	**Severity**	INFO	**Parameters**	Primary Volume, Secondary Volume
Message	Snapshot volume pair **x/y** created				
Description	Snapshot volume pair **x/y** was created.				
Advice	None				

Event ID	0x3C01				
Type	SNAPSHOT	**Severity**	INFO	**Parameters**	Primary Volume, Secondary Volume
Message	Snapshot volume pair **x/y** deleted				
Description	Snapshot volume pair **x/y** was deleted.				
Advice	None				

Event ID	0x3C02				
Type	SNAPSHOT	**Severity**	INFO	**Parameters**	VVOL ID
Message	VVOL**x** created				
Description	Snapshot volume vvo**x** was created.				
Advice	None				

Event ID	0x3C03				
Type	SNAPSHOT	**Severity**	INFO	**Parameters**	VVOL ID
Message	VVOL**x** deleted				
Description	Snapshot volume vvo**x** was deleted.				
Advice	None				

Event ID	0x3C04				
Type	SNAPSHOT	**Severity**	ERROR	**Parameters**	Secondary volume
Message	Secondary volume **x** is out of free space				
Description	All space of the secondary volume was occupied. Some or all snapshot volumes on this secondary volume would become faulty.				
Advice	Delete all faulty snapshot volumes and expand the secondary volume to a reasonable large capacity to prevent data loss caused in the future.				

Event ID	0x3C05				
Type	SNAPSHOT	**Severity**	INFO	**Parameters**	Primary Volume, Secondary Volume
Message	Snapshot volume pair **x/y** imported				
Description	Snapshot volume pair **x/y** was imported.				
Advice	None				

Event ID	0x3C07				
Type	SNAPSHOT	**Severity**	WARNING	**Parameters**	Secondary Volume
Message	Secondary volume **x** is **y**% full				
Description	The percentage of used space on secondary volume exceeds the pre-defined threhold level.				

Advice	Consider to expand secondary volume to prevent data loss.

Event ID	0x3C08				
Type	SNAPSHOT	**Severity**	INFO	**Parameters**	Spare COW volume
Message	Spare COW volume **x** is added.				
Description	Spare COW volume **x** was added.				
Advice	None				

Event ID	0x3C09				
Type	SNAPSHOT	**Severity**	INFO	**Parameters**	Spare COW volume
Message	Spare COW volume **x** is removed.				
Description	Snapshot volume pair **x** was removed.				
Advice	None				

Event ID	0x3C0B				
Type	SNAPSHOT	**Severity**	INFO	**Parameters**	Primary volume, Snapshot volume
Message	Primary volume **x** is restoring to SVOL **y**.				
Description	Primay volume **x** was restoring to SVOL **y**.				
Advice	None				

Event ID	0x3C0C				
Type	SNAPSHOT	**Severity**	INFO	**Parameters**	Primary volume, Snapshot volume
Message	Restoring task from primary volume **x** to SVOL **y** is done.				
Description	Restoring task from primary volume **x** to SVOL **y** was done.				
Advice	None				

Index

A

accessing the RAID GUI **2-1**
add LUNs in host **2-39**
add LUNs in storage group **2-41**
array recovery **2-52**
  faulty **2-52**
  optimal **2-52**
  partition state transition **2-53**
array roaming **2-51**
auto logout
  setting **2-72**
auto spare **2-55**
auto write-through cache **2-67**
automatic resume **2-48**
AV streaming **2-19**

B

background task messages **3-4**
bad block alert
  setting **2-57**
bad block clone
  setting **2-58**
beeper alarm **6-1**
beeper control **2-67**
bind host/host group and storage group **2-42**
boot utility **C-1**
  set IP address **C-2**
  set password **C-5**
  update boot ROM **C-4**
  update system ROM **C-4**

C

change password **2-72**
check on read **2-30**
cloning **2-47**
  automatic resume **2-48**
COM port setting **2-60**
concatenating striping member volumes **1-9**
concatenating volume units **1-9**, **2-47**
controller
  factory setting **2-68**

D

disk group
  creating **2-25**
  defined **1-9**
  defragmenting **2-43**
  deleting **2-26**
  expanding **2-43**
disk self test (DST) **2-50**
  restrictions **2-50**
DiskPart utility **5-48**
  extend partition **5-56**
  shrink partition **5-56**

E

emergent info **3-4**
enclosure polling interval **2-75**
erase HDD configurations **2-68**
erase NVRAM configurations **2-68**
event log messages **D-1**
expanding logical disks **2-34**, **2-45**, **2-46**
expanding volumes **2-46**
extensive supportive tools **B-13**

F

fast read response **2-30**
FC port
  connection mode
    auto, arbitration loop, fabric **2-60**
  setting **2-59**
forgotten password **2-11**

G

global spare
  defined **1-9**
GUI refresh rate **2-75**

H

HDD mode, defined **2-21**
HDD state, defined **2-21**
HDD state, tray color **2-7**
HDD, cloning **2-47**
HDD, code **2-6**

I

intelligent data computation **2-30**
interface features
  administration access control **B-15**
  CLI commands **B-14**
  remote management via web,

telnet, and SSH **B-15**
web-based GUI **B-14**
web-based GUI over PPP **B-15**
IO queue, NCQ **2-58**

J

JBOD
creating **2-23**
creating volume pair **2-24**
deleting **2-23**
JBOD, defined **A-12**
spanned disk array without fault tolerance **A-12**

L

language **2-1**
LCD console
background task messages **3-4**
creating a RAID array **3-6**
emergent info **3-4**
ethernet setting **3-7**
hotkeys **3-5**
status info **3-3**
terminal port setting **3-7**
LCD manipulation procedure **3-1**
LD read algorithm
check on read **2-30**
fast read response **2-30**
intelligent data computation **2-30**
local spare
defined **1-9**
logical disk
creating **2-27**
creating volume pair **2-30**
defined **1-9**
deleting **2-29**
expanding **2-34**, **2-45**, **2-46**
shrinking **2-46**
logical unit
defined **1-9**
login **2-11**
LUN mapping **1-10**
defined **1-10**

M

management tool
VDS provider **5-73**
maximum IO per second **2-19**
maximum throughput **2-19**
member disk
defined **1-9**
meta-data update frequency **2-56**
migrating **2-44**
limitations **2-44**
mirror write cache **5-23**
setting **5-25**
mode
config mode **2-18**
monitor mode **2-5**
switch mode **2-6**
MPIO (multi-path IO) **2-38**
MPIO device
add new logical disks **5-76**
MPIO device information page **5-10**
MPIO driver installation **5-8**
MPIO host
configuring **5-2**
MPIO policy
settings **5-11**
path policy **5-11**
preferred working path **5-11**
switch counter **5-12**
weight mode **5-11**
MPIO policy settings **5-11**
MTID **5-18**
Multiple ID **5-18**
multiple system viewer **2-3**

N

NRAID, defined **A-13**

O

on-line array roaming control **2-56**

P

partition state transition **2-53**
password settings **3-8**
path failover alert delay **2-67**
PathGuard
uninstalling **5-8**
PathGuard MPIO
configuration
dual independent MPIO hosts **5-4**
multipath clustered servers **5-6**
PathGuard MPIO utility
add MPIO host
remote **5-15**
benefits **5-1**
performance profile **2-19**
AV streaming **2-19**
maximum IO per second **2-19**
maximum throughput **2-19**
PPP port setting **2-61**

R

RAID 0, defined **A-3**
  striped disk array without fault tolerance **A-3**
RAID 1, defined **A-4**
  mirroring **A-4**
RAID 10, defined **A-8**
  high reliability setup combined with high performance **A-8**
RAID 3, defined **A-5**
  parallel transfer with parity **A-5**
RAID 30, defined **A-9**
  byte striping with parity combined with block striping **A-9**
RAID 5, defined **A-6**
  independent data disks with distributed parity blocks **A-6**
RAID 50, defined **A-10**
  block striping with distributed parity combined with block striping **A-10**
RAID 6, defined **A-7**
  independent data disks with double parity blocks **A-7**
RAID 60, defined **A-11**
  striping with dual parity **A-11**
RAID system, redundant
  rear view **2-9**, **2-10**
RAID system, single
  rear view **2-9**
RAID, quick setup **2-20**
RAIDGuard central
  features and benefits **5-58**
recovery, procedures **2-53**
redundant controller **5-21**
  active-active mode **5-25**
    dual independent mpio hosts **5-29**
    dual mpio clustering hosts **5-31**
    single mpio host (dual channel) **5-25**
    single mpio host (quad channel) **5-26**
  active-passive mode
    single mpio host (dual channel) **5-33**
  controller failback **5-36**
  controller failover **5-35**
  data synchronization **5-34**
  notification messages **5-37**
  path failback **5-35**
  setting the preferred controller **5-25**
regenerating parity **2-50**
remove LUNs from host **2-40**
remove LUNs in storage group **2-42**
restoring to factory settings **2-68**
RGC
  components
    RAIDGuard Central Agent (RGC Agent) **5-59**
    RAIDGuard Central GUI (RGC GUI) **5-59**
    RAIDGuard Central Server (RGC Server) **5-59**
  deployment procedures **5-60**
  installing **5-61**
  launching GUI **5-62**
    login **5-65**
    main screen **5-65**
  MSN event notification
    configuring **5-72**
  RAID system monitoring **5-71**
    export event logs **5-72**
    launch RAID system GUI **5-72**
    view event logs **5-71**
  RAID system registration **5-67**
  uninstalling **5-62**
RS232 COM port
  setting **C-1**

S

SAS enclosure **2-12**
SAS JBOD chassis
  monitor mode **2-16**
  rear view **2-13**
scrubbing **2-49**
  restrictions **2-49**
send a test mail **2-66**
setting up the network **2-70**
  DHCP **2-70**
  static **2-70**
setting up the time **2-71**
shrinking logical disks **2-46**
shrinking volumes **2-47**
SMART polling **2-57**
SMTP **2-61**
  setting **2-61**
  test SMTP server **2-71**
snapshot
  features **5-38**
snapshot volume
  creating **5-48**
  restoring **5-41**
SNMP
  send a test SNMP trap **2-63**
  setting **2-62**
spare restore **2-55**

SSL forced
setting **2-73**
status info **3-3**
storage provisioning **2-36**
selective storage
add hosts **2-41**
add LUNs in storage group **2-41**
bind host/host group and storage group **2-42**
remove hosts **2-41**
remove LUNs in storage group **2-42**
unbind hosts/ host groups and storage groups **2-42**
simple storage
add LUNs in a storage port **2-36**
remove LUNs in storage port **2-38**
symmetric storage
add hosts **2-38**
add LUNs in host **2-39**
remove hosts **2-39**
remove LUNs from host **2-40**
Symmetric
MPIO (multi-path IO) **2-38**

T

test SMTP server **2-71**

U

unbind hosts/ host groups and storage groups **2-42**
update boot code **2-74**
update firmware **2-74**
UPS
setting **2-66**

V

VDS provider
configuration utility **5-74**
installing **5-74**
uninstalling **5-74**
virtual volume
creating **2-35**
deleting **2-36**
volume pair
automatic expansion **2-34**
creating **2-34**
setting overflow alert **2-34**
volume
concatenated striping **1-9**
concatenating **1-9**, **2-47**
creating **2-31**
restrictions **2-31**
creating volume pair **2-33**
defined **1-9**
deleting **2-32**
expanding
restrictions **2-46**
shrinking **2-47**
restrictions **2-47**
striping **1-9**

W

write completion
write-behind **2-38**, **2-40**, **2-42**
write-through **2-38**, **2-40**, **2-42**
write log control **2-56**